Introduction au groupe de Brauer

Julien Soumier, Nicolas Doineau

Octobre 2021

Projet de recherche, Master 2 agrégation

Motivations

Lors de notre précédent projet, nous nous sommes intéressés à un principe *local global* : le théorème de Hasse-Minkowski. L'idée est la suivante. En décomposant un problème global (la recherche de zéros d'une forme quadratique sur $\mathbb{Q}$) en plusieurs problèmes locaux plus simples que l'on sait résoudre (la même recherche mais sur sur les complétés de $\mathbb{Q}$), on sait remonter à la résolution du problème global. Nous avons trouvé ce principe absolument magnifique, et nous souhaitons en apprendre davantage. En parcourant la littérature sur le sujet, on trouve beaucoup de références au principe *d'obstruction de Brauer-Manin*. Il semblerait que l'une des clés pour appréhender les principes locaux-globaux, résiderait dans la structure d'un groupe, appelé *groupe de Brauer*. Ce projet a donc pour but de découvrir celui-ci. Nous en verrons deux constructions qui reposent sur des bases a priori différentes, bien que nous démontrerons leur équivalence, a posteriori.

Table des matières

1 Notions de théorie des catégories

Dans les différentes branches des mathématiques, et dépendant des objets que l'on manipule, on voit apparaître une sorte de "méta-structure". Prenons l'exemple fondamental des groupes. Lorsque l'on étudie ces objets, on a intuitivement envie de pouvoir passer d'un groupe à l'autre, par des "fonctions qui respectent la structure". De là naît la notion d'homomorphisme de groupe. De même en topologie, les applications que l'on a envie d'utiliser sont les fonctions continues, principalement à cause de l'équivalence bien connue pour $f : A \to B$, f est continue sur A si et seulement si pour tout O ouvert de B, $f^{-1}(O)$ est ouvert dans A. La théorie des catégories a pour objectif de généraliser cette "méta-structure". L'idée est surtout d'étudier les relations entre les objets afin d'obtenir des informations sur ces derniers, plutôt que d'étudier les objets directement. Dans ce chapitre certaines démonstrations seront passées sous silence, nous donnerons cependant des références explicites où trouver les détails.

1.1 Catégories

Définition 1.1. *Une catégorie $\mathscr{C}$ est la donnée de :*

- *Une classe $Obj(\mathscr{C})$, dont les éléments seront les* objets *de la catégorie*
- *Pour toute pair d'objet (A, B) ordonnée, un ensemble $Hom_{\mathscr{C}}(A, B)$ de* morphismes, *dont les éléments seront notés $f : A \to B$*
- *Pour tout objet A, un* morphisme identité *élément de $Hom_{\mathscr{C}}(A, A)$ noté id_A*
- *Une* loi de composition, *pour tout triplé (A, B, C) ordonné :*

$$\circ : Hom_{\mathscr{C}}(A, B) \times Hom_{\mathscr{C}}(B, C) \to Hom_{\mathscr{C}}(A, C)$$

- *Le tout vérifiant : pour tout objets A, B, C, D, et morphismes $f : A \to B$, $g : B \to C$ et $h : C \to D$:*

$$(h \circ g) \circ f = h \circ (g \circ f)$$
$$id_B \circ f = f = f \circ id_A$$

Remarque-définition : Lorsque $Obj(\mathscr{C})$ est un ensemble, on parlera de petite catégorie.

Des questions très profondes se posent quant à cette définition. Qu'est-ce qu'une classe ? Dans quelle mesure pouvons nous les manipuler comme si il s'agissait d'ensembles ? Dans le cadre de ce projet nous laisserons de côté ces préoccupations, et nous demandons aux logiciens de bien vouloir nous en excuser.

Nous parlerons d'isomorphisme lorsqu'un morphisme possède un même inverse à gauche et à droite pour la loi de composition. Cela coïncide très souvent avec les notions connues.

Exemple 1. Une catégorie élémentaire est celle des ensembles, notée **Ens**. Ces objets sont bien entendu les ensembles (c'est pour de tels exemples que l'on prend une "collection" dans la définition, l'ensemble des ensembles n'existant pas...) et les morphismes sont les fonctions.

Exemple 2. Comme annoncé précédemment on peut donc considérer entre autre la catégorie des groupes abéliens **Ab**. Les éléments sont donc les groupes abéliens, les morphismes sont les homomorphismes de groupes, le morphisme identité et la compositions sont ce dont on a l'habitude.

Exemple 3. Pour A un anneau (resp. commutatif) on peut introduire la catégorie des A-modules (resp. A-module à gauche), noté A-**Mod** (même notation si il n'y a pas d'ambiguïté). Comme précédemment les classes d'objets et de morphismes sont celles qui nous sont familières.

Exemple 4. Si on se donne une catégorie $\mathscr{C}$, on a un moyen d'en construire une autre : *la catégorie opposée* (ou duale) notée $\mathscr{C}^{op}$. Les objets de $\mathscr{C}^{op}$ sont ceux de $\mathscr{C}$. Et à tout morphisme $f : A \to B$ de $\mathscr{C}$, on associe $f^{op} : B \to A$ morphisme de $\mathscr{C}^{op}$. Il faut aussi veiller à "renverser" la loi de composition pour munir ces classes de la structure de catégorie.

Définition 1.2. *un morphisme $f : B \to C$ est un* monomorphisme *quand : Pour tout e_1, e_2 morphismes de A dans B, si on a $f \circ e_1 = f \circ e_2$ alors $e_1 = e_2$.*

On remarque que dans les catégories **Ab** et A-**mod**, les monomorphismes sont les morphismes injectifs au sens usuel, mais attention ce n'est pas toujours le cas.

Définition 1.3. *un morphisme $f : B \to C$ est un* épimorphisme *quand : Pour tout e_1, e_2 morphismes de C dans D, si on a $e_1 \circ f = e_2 \circ f$ alors $e_1 = e_2$.*

Encore une fois, dans les catégories **Ab** et A-**mod**, les épimorphismes sont les morphismes surjectifs, mais ce n'est toujours pas un fait général.

Exemple 5. Soit $\mathscr{C}$ une catégorie. Les monomorphismes de $\mathscr{C}$ sont les épimorphismes de $\mathscr{C}^{op}$, et inversement.

Maintenant souhaiterait voir si il y a des objets triviaux dans une catégories, comme par exemple dans la catégorie **Ab** on dispose du groupe $\{e\}$ constitué du neutre. Cette idée est motivée par l'envie de parler de noyaux et de conoyaux de morphismes.

Définition 1.4. *On considère une catégorie $\mathscr{C}$, et I, T des objets de $\mathscr{C}$.*

- *I est dit* initial *si pour tout objet B il existe un unique morphisme $f : I \to B$.*
- *T est dit* final *si pour tout objet B il existe un unique morphisme $f : B \to T$.*
- *Un objet à la fois initial et final est appelé un* objet zéro.

On remarque que tous les objet initiaux (resp. finaux) sont isomorphes, on se permettra donc de parler de **l**'objet initial, terminal ou zéro.

Exemple 6. Dans les catégories **Ab** et A-**mod** l'objet $0 = \{e\}$ est un objet zéro.

Dans la suite on suppose que l'on a une catégorie $\mathscr{C}$ qui possède un objet zéro noté 0.

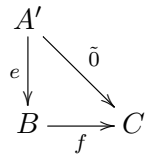
Exemple 7. Soit A, B des objets de $\mathscr{C}$. On a alors accès à un élément particulier de $Hom_{\mathscr{C}}(A, B)$, l'unique (par propriété de 0) application :

$$\tilde{0}_{A,B} : A \to 0 \to B$$

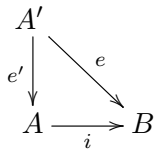
Si il n'y a pas d'ambiguité on notera simplement $\tilde{0}$. Il est important de remarquer que pour tout autre morphisme $g : B \to B$, on a l'égalité $g \circ \tilde{0} = \tilde{0}$. En effet si on note $g \circ \tilde{0} : A \to_{f_1} 0 \to_{f_2} B \to_g B$ où $f_2 \circ f_1 = \tilde{0}$ est l'unique factorisation de $\tilde{0}$. On a alors que $(g \circ f_2) \circ f_1$ est un morphisme de $A \to 0 \to B$. Donc par unicité on a $(g \circ f_2) \circ f_1 = g \circ \tilde{0}$.

Définition 1.5. *Soit $f : B \to C$ un morphisme de $\mathscr{C}$. Un noyau de f est un morphisme $i : A \to B$ tel que $f \circ i = \tilde{0}$ et qui vérifie la propriété universelle suivante : pour tout autre morphisme $e : A' \to B$ tel que $f \circ e = \tilde{0}$, il existe une unique factorisation $e' : A' \to A$ telle que $e = i \circ e'$.*

Visuellement on a les diagrammes commutatifs suivant :



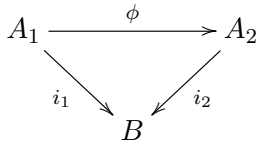
donne un unique e' tel que



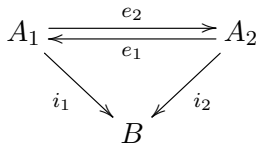
Proposition 1.1. *Soit $f : B \to C$ un morphisme de $\mathscr{C}$. Soit $i : A \to B$ un noyau de f. Alors i est un monomorphisme.*

Démonstration. Soit $f, g : A' \to A$ des morphismes de $\mathscr{C}$ vérifiant $i \circ g = i \circ h$. On remarque qu'alors $\tilde{0} = (f \circ i) \circ h = f \circ (i \circ h) = f \circ (i \circ g)$. Il existe alors par propriété universelle un unique $e' : A' \to A$ tel que $i \circ h = i \circ e'$, donc par unicité $e' = h$. Or $i \circ h = i \circ g = i \circ e'$ donc par unicité $e' = g$. Ainsi $g = h$. □

Proposition 1.2. *Soit $f : B \to C$ un morphisme de $\mathscr{C}$. Soit $i_1 : A_1 \to B$ et $i_2 : A_2 \to B$ des noyaux de f. Alors i_1 et i_2 sont isomorphes au sens suivant : Il existe un isomorphisme $\phi : A_1 \to A_2$ tel que $i_1 = i_2 \circ \phi$. C'est à dire faisant commuter le diagramme suivant :*



Démonstration. Par propriété universelle du noyau i_1 il existe un unique $e_1 : A_2 \to A_1$ tel que $i_2 = i_1 \circ e_1$. De même il existe un unique $e_2 : A_1 \to A_2$ tel que $i_1 = i_2 \circ e_2$. On a donc le diagramme suivant :



Il reste à voir que e_1 et e_2 sont des isomorphismes réciproques l'un de l'autre.

$$\begin{aligned} i_2 &= i_1 \circ e_1 && \textit{or } i_1 = i_2 \circ e_2, \textit{ donc} \\ i_2 &= i_2 \circ (e_1 \circ e_2) && \textit{donc par monomorphie} \\ id_{A_1} &= e_1 \circ e_2 \end{aligned}$$

Par le même raisonnement on obtient $id_{A_2} = e_2 \circ e_1$, donc i_1 et i_2 sont bien isomorphes. □

Ainsi on peut parler, quand il existe, **du** noyau $i : A \to B$ d'un morphisme $f : B \to C$. Le noyau étant un monomorphisme, on l'identifiera souvent (quand cela fait sens) au sous-objet $i(A)$ de B.

Exemple 8. Dans les catégories **Ab**, A-**mod** le noyau d'un morphisme $f : B \to C$ correspond à ce que l'on veut : $\{x \in A | f(x) = 0\}$.

Voici maintenant la notion duale du noyau, au même titre que l'épimorphie est la notion dual de la monomorphie.

Définition 1.6. *Soit $f : B \to C$ un morphisme de $\mathscr{C}$. Un conoyau de f est un morphisme $p : C \to D$ tel que $p \circ f = \tilde{0}$ et qui vérifie la propriété universelle suivante : pour tout autre morphisme $g : C \to D'$ tel que $g \circ f = \tilde{0}$, il existe une unique factorisation $g' : D \to D'$ telle que $g = g' \circ p$.*

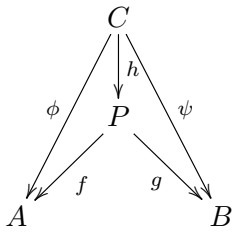
Proposition 1.3. *Les mêmes raisonnements que pour le noyau nous donne que conoyau est (quand il existe) un épimorphisme unique à isomorphisme près.*

Exemple 9. Les noyaux d'une catégorie sont les conoyaux de sa catégorie duale, et inversement.

Il est également naturel de vouloir à partir de deux objet dans une catégorie, créer un autre objet possédant des "bonnes propriétés". L'exemple que l'on veut suivre est celui du produit cartésien dont on a l'habitude ou de l'union disjointe.

Définition 1.7. *Produit*
Soit A, B deux objets d'une catégorie $\mathscr{C}$. Un produit *de A et B consiste en un triplet $(P, f : P \to A, g : P \to B)$ (d'un objet et de deux morphismes) vérifiant la propriété universelle suivante :*

Pour tout autre triplet $(C, \phi : C \to A, \psi : C \to B)$ il existe un unique morphisme $h : C \to P$ faisant commuter le diagramme suivant :

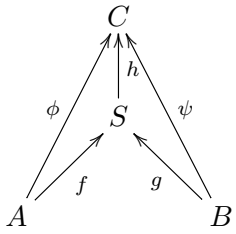


Exemple 10. On se place dans la catégorie **Ens**. Soit E et F deux ensembles, $X = E \prod F$ leur produit cartésien avec $p_E : X \to E$ et $p_F : X \to F$ les projections sur les facteurs respectifs. Alors (X, p_E, p_F) est un produit de E et F

On s'empresse de donner la version duale, toujours obtenue en renversant le sens des flèches :

Définition 1.8. *Coproduit (ou somme)*
Soit A, B deux objets d'une catégorie $\mathscr{C}$. Un coproduit *de A et B consiste en un triplet $(S, f : A \to S, g : B \to S)$ vérifiant la propriété universelle suivante :*

Pour tout tel autre triplet (C, ϕ, ψ) il existe un unique morphisme $h : S \to C$ faisant commuter le diagramme suivant :



Remarque On montre encore sans difficulté (l'unicité de h nous sauve) que deux produits (X, f, g), (X', f', g') (de même pour les coproduits) sont isomorphes, au sens où il existe un ismorphisme $\phi : X \to Y$, qui vérifie $f = f' \circ \phi$ et $g = g' \circ \phi$.

Il arrive régulièrement que ces notions soient isomorphes, mais nous prendrons tout de même soin de les noter de manière distincte, le produit sera noté $A \prod B$ et le coproduit $A \bigsqcup B$.

1.2 Catégories abéliennes

1.2.1 Généralités

On souhaiterait maintenant affiner la structure d'une catégorie. En effet dans la catégorie **Ab** par exemple, on a une structure de groupe abélien naturelle sur les $Hom(C, D)$. En outre il serait commode de pouvoir considérer des sommes (et donc des produits) des éléments eux même de la catégorie, comme le produit direct ou l'union disjointe dans les catégories que l'on a l'habitude de manier.

Définition 1.9. *Soit $\mathscr{C}$ une catégorie. $\mathscr{C}$ est une catégorie pré-additive quand tout $Hom(B, C)$ est muni d'une loi interne qui en fait un groupe abélien, et qui se distribue par rapport à la composition.*

Exemple 11. Si on prend $\mathscr{C}$ une catégorie pré-additive, et A, B, C, D des objets, f, g_1, g_2, h des morphismes tels que :

$$A \xrightarrow{f} B \underset{g_2}{\overset{g_1}{\rightrightarrows}} C \xrightarrow{h} D$$

Ayant une loi sur $Hom(B, C)$ on peut considérer $g_1 + g_2$, et on la distribution suivante :

$$h \circ (g_1 + g_2) \circ f = h \circ g_1 \circ f + h \circ g_2 \circ f$$

Proposition 1.4. *Considérons une catégorie pré-additive $\mathscr{C}$, qui possède un 0, ainsi que A_1, A_2 deux objets de $\mathscr{C}$. Si il existe A dans $obj(\mathscr{C})$ et des morphismes vérifiant :*

- *Pour $i = 1, 2$ on a , $\phi_i : A_i \to A$, $\pi_i : A \to A_i$ avec $\pi_i \circ \phi_i = Id_{A_i}$ et $\pi_i \circ \phi_j = 0 \quad (i \neq j)$.*

Alors on a équivalence entre les trois énoncés ci-dessous :

i) $\phi_1 \circ \pi_1 + \phi_2 \circ \pi_2 = Id_A$

ii) *A est le produit $A = A_1 \prod A_2$*

iii) *A est le coproduit $A = A_1 \bigsqcup A_2$*

Définition 1.10. *Avec les mêmes notations que ci-dessus, dans le cas où une des propriétés équivalentes est vérifiée, on dit que A est le* biproduit *de A_1 et A_2, et on le note $A = A_1 \bigoplus A_2$*

En itérant, on voit que l'on est capacité de construire un biproduit d'une famille finie d'éléments de $\mathscr{C}$, de plus le biproduit d'objet lorsqu'il existe, est unique à isomorphisme près.

Définition 1.11. *Soit $\mathscr{C}$ une catégorie. $\mathscr{C}$ est une catégorie additive quand :*

- *$\mathscr{C}$ est pré-additive (quelle surprise...)*
- *$\mathscr{C}$ possède un élément 0 nul.*
- *Tout couple d'objets (A, B) admet un biproduit $A \bigoplus B$*

Proposition 1.5. *Dans une telle catégorie $\mathscr{C}$ additive, pour deux objets A, B, l'élément nul de $Hom(A, B)$ (voir exemple 7) est précisément l'élément neutre pour la loi de groupe abélien.*

Démonstration. On note $\tilde{0}$ l'élément nul de $Hom(A, B)$ et e le neutre pour "+". On a vu que pour tout $g : B \to B$, $g \circ \tilde{0} = \tilde{0}$. En particulier :

$$\begin{aligned} \tilde{0} &= \tilde{0} \circ (Id_B + Id_B) \\ &= (\tilde{0} \circ Id_B) + (\tilde{0} \circ Id_B) \\ &= \tilde{0} + \tilde{0} \\ &\text{d'où} \\ e &= \tilde{0} \end{aligned}$$

□

Cette identification est la bienvenue, en effet elle nous permet de mieux appréhender la notion de mono-(ou épi)morphisme :

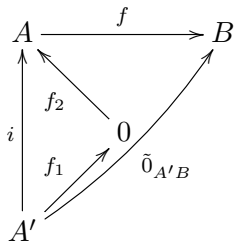
Proposition 1.6. *Soit $\mathscr{C}$ une catégorie additive, deux éléments A, B, et $f : A \to B$.*

i) *f est un monomorphisme si et seulement si le noyau de f est $0 \to A$.*

ii) *f est un épimorphisme si et seulement si le conoyau de f est $B \to 0$.*

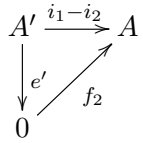
Démonstration. Démontrons (i), et (ii) en découlera par dualité, c'est à dire passage à la catégorie opposée.

Si $f : A \to B$ est un monomorphisme, on note f_2 l'unique $0 \to A$. On remarque en premier lieu qu'on a bien $f \circ f_2 = \tilde{0}$. Soit A' un objet de $\mathscr{C}$ et $i : A' \to A$ tel que $f \circ i = \tilde{0}_{A'A}$. Faisons un diagramme pour introduire les notations :



On remarque alors que $f \circ i = \tilde{0}_{A'B} = f \circ \tilde{0}_{A'A}$, et comme f est un monomorphisme : $i = \tilde{0}_{A'A}$. Ainsi i se factorise de manière unique par f_2. Donc f_2 est bien le noyau de f.

Si maintenant $f_2 : 0 \to A$ est le noyau de f. Soit $i_1, i_2 : A' \to A$, tels que $f \circ i_1 = f \circ i_2$. Alors comme $\mathscr{C}$ est abélienne $f \circ (i_1 - i_2) = \tilde{0}_{A'B}$. Donc $i_1 - i_2$ se factorise uniquement par $f_2 : 0 \to A$, il existe $e' : A' \to 0$ tel que le diagramme suivant commute :



Donc $i_1 - i_2 = \tilde{0}_{A'A}$ par unicité, et donc $i_1 = i_2$. □

On y est presque ! Il nous reste plus qu'à nous assurer que dans les catégories que nous verrons, il est toujours possible de parler du noyau ou conoyau d'un morphisme. Ceci se révèle particulièrement important car on souhaite pouvoir partir à la "chasse au diagramme", afin de récolter un maximum d'information sur les relations entre les objets.

Définition 1.12. *Soit $\mathscr{C}$ une catégorie, elle sera* abélienne *quand :*

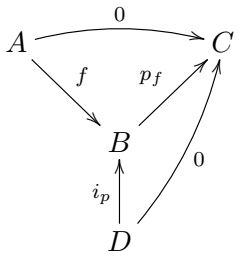
- *$\mathscr{C}$ est additive*
- *Tout morphisme admet un noyau et un conoyau*
- *Tout monomorphsime est le noyau de son conoyau*
- *Tout épimorphisme est le conoyau de son noyau*

Ceci donne en particulier que dans une catégorie abélienne, les morphismes que sont des bijections sont des isomorhismes. Ce qui n'est pas toujours évident, comme lorsqu'on considère les espaces topologiques, une bijection continue n'est pas automatiquement un homéomorphisme.

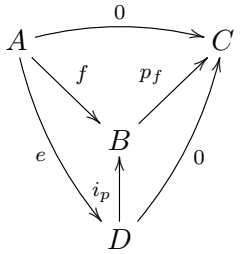
On peut également remarquer que la définition est "invariante par dualité", ce qui nous donne : si $\mathscr{C}$ est abélienne alors $\mathscr{C}^{op}$ est abélienne. Dans la suite $\mathscr{C}$ désigne une catégorie abélienne.

Proposition 1.7. *Soit $f : A \to B$ un morphisme de $\mathscr{C}$, alors f se factorise : $f = m \circ e$ avec m un monomorphisme.*

Démonstration. L'idée est de prendre $m = Ker(coKer(f))$. Notons donc $p_f : B \to C$ le conoyau de f et $i_p : D \to B$ le noyau de p_f.Ces derniers existent car $\mathscr{C}$ est abélienne. On a alors le diagramme commutatif suivant :



Ainsi par factorisation de f par le noyau i_p, il existe un $e : A \to D$ faisant commuter le diagramme :



Comme $m = i_p$ est le noyau d'un morphisme, on sait que c'est un monomorphisme. □

Définition 1.13. *Soit $f : A \to B$ un morphisme de $\mathscr{C}$, alors le monomorphisme $Im(f) := Ker(Coker(f))$ ayant la propriété précédente est appelé* image *de f.*

En restant volontairement vague, on peut montrer que dans ces catégories abéliennes, tout ce passe *localement* comme prévu. On peut définir, comme on s'y attendrai dans la catégorie des R-modules, des quotients et des sous-objets, qui intuitivement correspondent à ce que l'on s'imagine. C'est ce qu'exprime entre autre le théorème de la section suivante.

1.2.2 Deux mots sur le théorème de Freyd–Mitchell

Définition 1.14. *Un foncteur $F : \mathscr{C} \to \mathscr{D}$ est dit fidèle (resp. plein) si pour tous objets C et C' de la catégorie $\mathscr{C}$ l'application $Hom_{\mathscr{C}}(C, C') \to Hom_{\mathscr{D}}(FC, FC')$ sont toutes des injections (resp. surjections)*

Théorème 1.1 (Freyd-Mitchell)**.** *[Wei][P.25] Soit $\mathscr{A}$ une petite catégorie abélienne, il existe un anneau R, unitaire, et un foncteur $F : \mathscr{A} \to R$-**mod** exact, fidèle et plein.*

Ce théorème va nous permettre de considérer dans la suite que nous ne travaillons que dans des catégories du type R-**mod** lorsque l'on manipule des catégories abéliennes.

1.2.3 Lemme du serpent

Le lemme considéré dans cette partie est fondamental, bien qu'il ne s'agisse en réalité que d'une chasse au diagramme. Le fait est que cette propriété, simple en apparence, nous permettra de construire le foncteur dérivé de manière très générale. Étudions dans un premier temps le cas des A-modules :

Proposition 1.8. *On considère le diagramme commutatif suivant dans la catégorie A-**mod** :*

$$\begin{array}{ccccccccc} & & A' & \xrightarrow{\alpha} & B' & \xrightarrow{p} & C' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow[\beta]{} & C & & \end{array}$$

En supposant les lignes exactes. On obtient alors un morphisme δ donnant la suite exacte :

$$ker(f) \longrightarrow ker(g) \longrightarrow ker(h) \xrightarrow{\delta} coker(f) \longrightarrow coker(g) \longrightarrow coker(h)$$

Démonstration. Il suffit d'écrire le diagramme complet en jeu :

$$\begin{array}{ccccccccc} & & ker(f) & \longrightarrow & ker(g) & \longrightarrow & ker(h) & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & A' & \xrightarrow{\alpha} & B' & \xrightarrow{p} & C' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow[\beta]{} & C & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & coker(f) & \longrightarrow & coker(g) & \longrightarrow & coker(h) & & \end{array}$$

Ainsi la façon naturelle de construire le morphisme voulu est :

$$\delta : \left\{ \begin{array}{rcl} ker(h) & \to & coker(f) \\ c & \mapsto & i^{-1}(g(p^{-1}(c))) \end{array} \right.$$

Il reste juste à vérifier qu'il est bien défini. Soit $c \in ker(h)$. Comme p est surjectif on peut prendre UN (pas forcément un seul...) élément $p^{-1}(c) \in B'$. On le fait descendre par g : $z := g(p^{-1}(c)) \in B$. Par commutativité du diagramme $h \circ p = \beta \circ g$, et donc $\beta(z) = 0$. Ainsi $z \in ker(\beta)$ et donc par exactitude d $z \in Im(i)$. Il existe alors un (et un seul cette fois par injectivité de i) élément $x \in A$ tel que $x = i^{-1}(g(p^{-1}(c)))$. Il ne reste plus qu'à vérifier que le choix de $p^{-1}(c)$ conserve la classe de x mod $Im(f)$. Si on a $z_0, z_1 \in B'$ tels que $p(z_0) = p(z_1) = c$, alors $z_0 - z_1 \in Ker(p)$ donc par exactitude $z_0 - z_1 \in Im(\alpha)$. Ainsi il existe $a \in A'$ tel que $\alpha(a) = z_0 - z_1$. Ainsi on a :

$$g(z_0) - g(z_1) = g(z_0 - z_1) = g \circ \alpha(a) = i \circ f(a)$$

Et donc

$$i^{-1}(g(z_0)) - i^{-1}(g(z_1)) = f(a) \quad \text{donc} \quad i^{-1}(g(z_0)) = i^{-1}(g(z_0)) \ \text{mod}\ Im(f)$$

Ainsi notre application δ est bien définie. □

Ceci reste vrai dans une catégorie abélienne quelconque, et c'est le théorème de Freyd-Mitchell qui nous permet de transférer le lemme précédent de la catégorie A-**mod** à une catégorie abélienne $\mathscr{C}$ quelconque.

En effet si on prend le même énoncé dans $\mathscr{C}$ quelconque, il suffit de considérer la plus petite sous-catégorie abélienne de $\mathscr{C}$ contenant les objets et morphismes du diagramme en question. On note cette dernière $\mathscr{S}$. Il est alors direct de voir que les objets de cette sous-catégorie forment un ensemble, on plonge donc $\mathscr{S}$ dans un catégorie A-**mod** pour un certain A, et on conclut par le lemme précédent.

1.3 Foncteurs

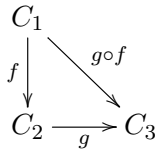
Une fois la notions de catégorie définie, on garde en tête notre idée de vouloir passer d'un objet à un autre en respectant la structure. On veut alors définir ce genre d'application pour la structure de catégorie, on les appelle les foncteurs.

Définition 1.15. *Soit $\mathscr{C}$ et $\mathscr{D}$ deux catégories. Un foncteur de $\mathscr{C}$ vers $\mathscr{D}$ est une "correspondance" qui vérifie :*

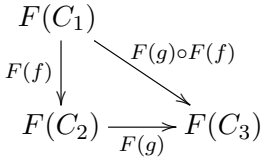
- *A tout C objet de $\mathscr{C}$, est associé un objet $F(C)$ de $\mathscr{D}$.*
- *A tout C_1, C_2 objets de $\mathscr{C}$, et tout morphisme $f : C_1 \to C_2$ de $Hom_{\mathscr{C}}(C_1, C_2)$, est associé un morphisme $F(f)$ de $Hom_{\mathscr{D}}(F(C_1), F(C_2))$.*
- *Pour tout C_1, C_2, C_3 objets, et $f : C_1 \to C_2$ $g : C_2 \to C_3$ morphismes de $\mathscr{C}$ on a*

$$\begin{aligned} F(g \circ f) =& F(g) \circ F(f) \\ F(id_{C_1}) =& id_{F(C_1)} \end{aligned}$$

En terme de diagramme commutatif on peut le visualiser comme ceci :



donne



Si on a l'idée folle de considérer la catégorie des catégories, on pourrait voir les foncteurs comme les morphismes de cette catégorie.

Exemple 12. Soit A un anneaux commutatif et M un A-module. Pour tout A-module N, les propriétés du produit tensoriel font de $M \otimes_A N$ un groupe abélien. La propriété universelle de $\otimes$ fait de l'application $F : N \mapsto M \otimes_A N$ un foncteur de la catégorie A-**mod** dans **Ab**.
En effet prenons M_1, M_2 des A-modules, et $f : M_1 \to M_2$ un morphisme de A-module. En considérant l'application bilinéaire

$$\begin{array}{ccc} N \times M_1 & \to & N \otimes_A M_2 \\ (x, y) & \mapsto & x \otimes_A f(y) \end{array}$$

la propriété universelle nous donne un unique morphisme de A-module :

$$\tilde{f} : N \otimes_A M_1 \longmapsto N \otimes_A M_2$$

telle que $\tilde{f}(x \otimes_A y) = x \otimes_A f(y)$. On a notre $F(f) = \tilde{f}$. On vérifie facilement que F respecte l'identité et la composition.

Définition 1.16. foncteur contravariant *Soit $\mathscr{C}$ et $\mathscr{D}$ deux catégories. Un foncteur contravariant G de $\mathscr{C}$ vers $\mathscr{D}$ est un foncteur de $\mathscr{C}^{op}$ dans $\mathscr{D}$.*

Remarque Un tel foncteur G associe donc à $f : A \to B$ un morphisme $G(f) : G(B) \to G(a)$ et on a $G(g \circ f) = G(f \circ g)$.

Exemple 13. Soit A un anneau, on se place dans A-**Mod**. Soit M un A-module. La correspondance $X \mapsto Hom(X, M)$ est un foncteur contravariant de A-**Mod** dans **Ab**. Soit N_1, N_2 deux A-modules et $f : N_1 \to N_2$. Alors le morphisme associé à f par le foncteur contravariant F est :

$$\begin{array}{ccc} F(f) : Hom(N_2, M) & \to & Hom_G(N_1, M) \\ g & \mapsto & g \circ f \end{array}$$

Définition 1.17. *Soit F un foncteur d'une catégorie $\mathscr{C}_1$ dans une catégorie $\mathscr{C}_2$. Soit une suite exacte :*

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

F est dit exact à gauche *quand*

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

est encore exacte. F est dit exact à droite *quand*

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

est encore exact, et F est dit exact quand il est exact à gauche et à droite.

Exemple 14. Reprenons l'exemple 12, et montrons que $F : N \mapsto N \otimes_A M$ un foncteur exact à droite. ($N \otimes_A M \cong M \otimes_A N$).

Soit

$$N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3 \longrightarrow 0$$

une suite exacte de A-module. On a alors la suite :

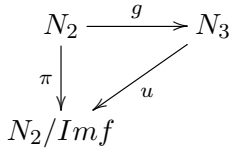
$$N_1 \otimes_A M \xrightarrow{\tilde{f}} N_2 \otimes_A M \xrightarrow{\tilde{g}} N_3 \otimes_A M$$

On voit que $\tilde{g}$ reste surjective car $N_3 \otimes_A M$ est engendré par les $n_3 \otimes m$. En effet pour $(n_3, m) \in N_3 \times M$, il existe par surjectivité de g un $n_2 \in N_2$ tel que $g(n_2) = n_3$, et donc $\tilde{g}(n_2 \otimes m) = g(n_2) \otimes m = n_3 \otimes m$.

En outre il est clair que l'on conserve $Im(\tilde{f}) \subset Ker(\tilde{g})$, car $(\tilde{g} \circ \tilde{f})(n_1 \otimes m) = (g \circ f)(n_1) \otimes m = 0 \otimes m$. Montrons que $Ker(\tilde{g}) \subset Im(\tilde{f})$. D'après ce que l'on vient de voir, on peut factorisé $\tilde{g}$ en :

$$\tilde{g_0} : N_2 \otimes_A M/\tilde{f}(N_1 \otimes_A M) \to N_3 \otimes_A M$$

Il suffit donc de voir que $\tilde{g_0}$ est injective, et pour montrer cela nous allons construire un inverse à gauche de $\tilde{g_0}$. On remarque en premier lieu que la suite exacte dans A-**Mod** nous donne un isomorphisme $u : N_3 \to N_2/Im(f)$ qui fait commuter le diagramme suivant : (π la projection canonique)



De plus si $z \in N_2 \otimes_A M$, on note $\bar{z}$ sa classe dans $N_2 \otimes_A M/\tilde{f}(N_1 \otimes_A M)$. Pour $n_3 \in N_3$ et $m \in M$ l'élément $u(n_3) \otimes m$ est bien définie modulo $\tilde{f}(N_1 \otimes_A M)$ car $u(n_3)$ l'est modulo $f(N_1)$.

On peut donc définir par propriété du produit tensoriel l'application :

$$\begin{array}{ccc} \phi : N_3 \otimes M & \to & N_2 \otimes_A M/\tilde{f}(N_1 \otimes_A M) \\ (n_3, m) & \mapsto & \overline{u(n_3) \otimes m} \end{array}$$

On a alors pour $(n_2; m) \in N_2 \times M$:

$$\phi \circ \tilde{g_0}(\overline{n_2 \otimes m}) = \phi \circ \tilde{g}(n_2 \otimes m) = \phi(g(n_2) \otimes m) = \overline{u(g(n_2)) \otimes m}$$

Or par définition on a $u(g(n_2)) = \pi(n_2)$ donc $\overline{u(g(n_2)) \otimes m} = \overline{n_2 \otimes m}$. Ainsi on a

$$\phi \circ \tilde{g_0} = Id.$$

De ce fait $\tilde{g_0}$ est injective, donc $Ker(\tilde{g}) \subset Im(\tilde{f})$ et enfin $Ker(\tilde{g}) = Im(\tilde{f})$ et F est un foncteur exact à droite.

Définition 1.18. *Dans une catégorie abélienne, un foncteur F est dit* additif *si pour tout objet A, B, l'application*

$$\begin{aligned} Hom(A,B) &\to Hom(F(A),F(B)) \\ f &\mapsto F(f) \end{aligned}$$

est un morphisme de groupe abélien. Donc $F(f+g) = F(f) + F(g)$.

On considère maintenant deux foncteurs F, G d'une catégorie $\mathscr{C}$ dans $\mathscr{D}$. On souhaite comprendre comment ils interagissent entre eux. On introduit alors la notion suivante :

Définition 1.19. *Une transformation naturelle.*
Une Une transformation naturelle *de F sur G, notée $\mu : F \to G$ et une correspondance telle que : A tout objet C de $\mathscr{C}$ on associe un morphisme $\mu_C : F(C) \to G(C)$ faisant commuter le diagramme suivant, pour tout $f : C \to C'$ morphisme de $\mathscr{C}$:*

$$\begin{array}{ccc} F(C) & \xrightarrow{F(f)} & F(C') \\ {\scriptstyle \mu_C}\downarrow & & \downarrow{\scriptstyle \mu_{C'}} \\ G(C) & \xrightarrow{G(f)} & G(C') \end{array}$$

2 Notions de cohomologie

Cette théorie de l'homologie, va nous permettre de "mesurer" le défaut d'exactitude de certaines suite. Nous nous attarderons ensuite sur le cas particulier de la cohomologie des groupes.

2.1 La catégorie des G-modules

Dans toute la suite, on note G un groupe noté multiplicativement.

Définition 2.1. G-module
Le triplet $(A, +, .)$ est un G-module quand on a :

- $(A, +)$ *est un groupe abélien*
- $. : (g, x) \mapsto g.x$ *est une action de G sur A*
- *Pour tout $g \in G$, l'application $\phi_g : x \mapsto g.x$ est un automorphisme du groupe abélien A.*

Remarque : On voit que se donner une structure de G-module sur un groupe abélien A, revient à se donner un morphisme :

$$\phi : \left\{ \begin{array}{ccc} G & \to & (Aut(A), \circ) \\ g & \mapsto & \phi_g \end{array} \right. .$$

Définition 2.2. G-morphisme
Soit A, A' deux G-modules. Soit $f : A \to A'$ est un morphisme de G-module *(ou un* G-morphisme*), quand c'est un morphisme de groupe entre A et A' et que :*

$$\forall (g, x) \in G \times A,\ f(g.x) = g.f(x)$$

On définit ainsi la catégorie des G-module notée $\mathbf{Mod}_G$, et l'ensemble des G-morphismes de A dans B sera noté $Hom_G(A, B)$. Une vérification rapide montre que c'est une catégorie abélienne.

Définition 2.3. *On note $\mathbb{Z}[G]$ l'algèbre du groupe G, c'est à dire l'ensemble :*

$$\mathbb{Z}[G] = \{\sum_{g \in F} n_g g\,;\ F \subset G\ fini\,,\ n_g \in \mathbb{Z}\}$$

muni de

$$\sum_{g \in F} n_g g + \sum_{g \in F'} n_g g = \sum_{g \in F \bigsqcup F'} n_g g$$

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

$\mathbb{Z}[G]$ est donc un anneau, mais attention si G n'est pas abélien, $\mathbb{Z}[G]$ n'est pas commutatif.

Remarque : On fixe A un groupe abélien. On voit que se donner une structure de G-module sur A, c'est se donner un module (à gauche) sur l'anneau $\mathbb{Z}[G]$.

En effet si A est un G-module on pose $\left(\sum_{g \in F} n_g g\right).x = \sum_{g \in F} n_g (g.x)$ bien défini car A est abélien. Réciproquement si A est un module sur l'anneau $\mathbb{Z}[G]$, alors il suffit de poser $g.x = gx$ (la somme réduite à $n_g g = 1g$).

Ainsi tout G-module est également un $\mathbb{Z}[G]$-module. Donc si on démontre des choses sur la catégorie A-**Mod** alors on en déduira des choses sur la catégorie $\mathbf{Mod}_G$, notamment le fait que $\mathbf{Mod}_G$ possède assez d'objets injectifs. On admet alors le théorème suivant, dont on trouve la démonstration dans [Wei], page 41.

Théorème 2.1. *Soit R un anneau. La catégorie R-**Mod** possède suffisament d'injectifs.*

Attardons nous sur un exemple particulier de foncteur additif exact à gauche, qui donnera naissance à la théorie cohomologique des groupes.

Théorème 2.2. *Soit A un G-module.*
On note A^G l'ensemble $\{a \in A | \forall g \in G\, g.a = a\}$ sous-groupe de A. Alors le foncteur :

$$F : \left\{ \begin{array}{rcl} \textbf{\textit{Mod}}_G & \to & \textbf{\textit{Ab}} \\ A & \mapsto & A^G \end{array} \right. .$$

est exact à gauche.

Démonstration. Premièrement il convient de vérifier rapidement que F est un foncteur. Soit A, C, B trois G-modules, et $f : A \to C$ et $g : C \to B$ deux G-morphismes. Le morphisme associé à f par F est :

$$\begin{array}{rcl} F(f) : A^G & \to & C^G \\ a & \mapsto & f(a) \end{array}$$

$F(f)$ est bien à valeur dans C^G car pour $a \in A^G$ on a $g.f(a) = f(g.a) = f(a)$, et c'est bien un morphisme de groupe abélien car f en est un. Il est alors clair que $F(id_A) = Id_{C^G} = Id_{F(A)}$ et que $F(g \circ f) = F(g) \circ F(f)$.

Deuxièmement, montrons que ce foncteur est exact à gauche (il est clairement additif), donnons nous une suite exacte de G-module :

$$0 \longrightarrow A \xrightarrow{f} C \xrightarrow{g} B$$

Comme f est injective, $F(f)$ l'est car c'est la restriction de f à A^G. Montrons que $Ker(F(g)) = Im(F(f))$. On a la suite d'équivalence :

$$\begin{aligned} c \in Ker(F(g)) &\iff c \in C^G \text{ and } F(g)(c) = 0 \\ &\iff c \in C^G \text{ and } g(c) = 0 \\ &\iff c \in C^G \text{ and } c \in Ker(g) \\ &\iff c \in C^G \text{ and } c \in Im(f) \\ &\iff c \in C^G \text{ and } \exists a \in A,\ f(a) = c \end{aligned}$$

Si on suppose que $c \in C^G$ et l'existence de $a \in A$ tel que $f(a) = c$.Montrons que $a \in A^G$. Soit $g \in G$. Alors

$$g.c = g.f(a) = f(g.a) = c = f(a)$$

Ainsi $f(g.a) = f(a)$ et par injectivité de f, on a bien $a = g.a$, donc $a \in A^G$. Et donc on a $c = f(a)$ avec $a \in A^G$ donc $c \in Im(F(f))$.

Inversement si $c \in Im(F(f))$ alors on a directement l'existence de $a \in A$ tel que $c = f(a)$ et donc on a par ce qui précède $c \in Ker(F(g))$.

Ainsi on a bien $F(f)$ injective, et $Ker(F(g)) = Im(F(f))$, donc on a la suite exacte suivante, et F est bien exact à gauche :

$$0 \longrightarrow F(A) \xrightarrow{F(f)} F(C) \xrightarrow{F(g)} F(B)$$

□

2.2 Complexes de chaînes

Nous pourrions nous placer dans le cadre général des catégories abéliennes, mais afin de faciliter les choses nous étudierons le cas particulier des G-modules. L'intérêt est que les noyaux, images et quotients de G-modules sont faciles à appréhender, car correspondent à ce dont nous avons l'habitude. Soit G un groupe. On se place dans la catégorie abélienne $\mathscr{C} = \mathbf{Mod}_G$.

Définition 2.4. *Complexe de chaîne. Soit $(E_i)_{i\in\mathbb{Z}}$ une famille d'objets de $\mathscr{C}$ et $(d^i : E^i \to E^{i+1})_{i\in\mathbb{Z}}$ une famille de morphismes. On dit alors que $((E^i)_i, (d^i)_i)$ est un* complexe de chaîne *quand pour tout $i \in \mathbb{Z}$, $d^{i+1} \circ d^i = 0$.*

$$\dots \xrightarrow{d^{i-1}} E^i \underbrace{\xrightarrow{d^i} E^{i+1} \xrightarrow{d^{i+1}} E^{i+2}}_{d^{i+1}\circ d^i = 0} \xrightarrow{d^{i+2}} \dots$$

On abregera "complexe de chaîne" en "complexe", et on notera (E, d) un complexe, avec $E = (E^i)_i$ et $d = (d^i)_i$. On remarque que l'on peut tout aussi bien considérer des complexes indexés par $\mathbb{N}$, c'est à dire des :

$$E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \xrightarrow{d^2} E^3 \xrightarrow{d^3} \dots$$

avec bien sur $i \in \mathbb{N}$, $d^{i+1} \circ d^i = 0$.

Définition 2.5. *Soit (E, d) un complexe.*

- *Les d^i sont appelés les* différentielles *du complexe*
- *Les noyaux $Ker(d^{i+1})$ sont appelés les* cycles *du complexe et notés Z^i (ou $Z^i(E)$ si il y a ambiguïté).*
- *Les images $Im(d^i)$ sont appelés les* bords *du complexe et notés B^i (ou $B^i(E)$ si il y a ambiguïté).*
- *Avec les précautions prises, on peut enfin définir le i-ème* groupe d'homologie $H^i(E) = Ker(d^{i+1})/Im(d^i) = Z^i/B^i$

On peut parler **du** i-ème groupe d'homologie car on a vu que les noyaux de morphismes sont isomorphes, et que l'on identifie le noyau de $f : A \to B$ avec le sous-objet sous-jacent de A. Les groupes d'homologie sont donc uniques à isomorphismes près, on notera alors $=$ pour "isomorphes". On notera $H(E)$ la famille $(H^i(E))_i$.

Exemple 1. Le complexe le plus simple à envisager est sûrement :

$$\dots \longrightarrow 0 \longrightarrow 0 \longrightarrow 0 \longrightarrow 0 \longrightarrow 0 \longrightarrow \dots$$

Exemple 2. Pour $i \in \mathbb{N}$, $E^i = \mathbb{Z}/8\mathbb{Z}$. On pose $E^{-1} = 0 = \{e\}$. On note $d^i : x \mapsto 4x$ (ou simplement d). On a alors la suite :

$$0 \longrightarrow \mathbb{Z}/8\mathbb{Z} \xrightarrow{d} \mathbb{Z}/8\mathbb{Z} \xrightarrow{d} \mathbb{Z}/8\mathbb{Z} \xrightarrow{d} \dots$$

Or on remarque que $d \circ d = 0$, et que d est un morphisme, donc on a bien défini un complexe de groupe On voit que pour $i \geq 1$ on a

$$H^i(E) = Ker(d_{i+1})/Im(d_i) = 2E^i/4E^i = \frac{2(\mathbb{Z}/8\mathbb{Z})}{4(\mathbb{Z}/8\mathbb{Z})} = \mathbb{Z}/2\mathbb{Z}$$

Définition 2.6. Morphisme de complexes
Un morphisme de complexe de degré r noté $f : (E', d') \to (E, d)$ est une famille de morphisme $f_i : E'^i \to E^{i+r}$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} E'^i & \xrightarrow{d'^i} & E'^{i+1} \\ {\scriptstyle f_i}\downarrow & & \downarrow{\scriptstyle f_{i+1}} \\ E^{i+r} & \xrightarrow[d^i]{} & E^{i+r+1} \end{array}$$

Quand on ne précise pas le degré d'un morphisme, il sera sous-entendu qu'il est de degré 0

Pour $f : E' \to E$ un morphisme de complexe, on a pour tout $i \in \mathbb{Z}$ un morphisme induit :

$$H^i(f) : H^i(E') \to H^i(E)$$

En effet prenons un $i \in \mathbb{Z}$.
Alors $f^i(Z^i(E')) \subset Z^i(E)$. En effet pour $y \in f^i(Z^i(E'))$ on a $x \in Z^i(E')$ tel que $f^i(x) = y$. Alors :

$$d^i(y) = d^i(f^i(x)) = f^{i+1}(d'^i(x)) = f^{i+1}(0) = 0$$

On peut donc définir $\bar{f}^i$: (π est la surjection canonique)

$$\begin{array}{ccc} Z^i(E') & \xrightarrow{f^i} & Z^i(E) \\ & {\scriptstyle \bar{f}^i}\searrow & \downarrow{\scriptstyle \pi} \\ & & Z^i(E)/B^i(E) \end{array}$$

De la même manière on montre que $f^i(B^i(E')) \subset B^i(E)$, ainsi $B^i(E') \subset Ker(\bar{f}^i)$ et donc $\bar{f}^i$ passe au quotient en l'application $H^i(f)$.

Ainsi lorsque l'on aura dans la suite un morphisme de complexe $f : E \to E'$, on notera $H(f)$ la famille de morphismes induit sur la famille d'homologie $H(E) \to H(E')$. Il est clair que de manière générale $H(f \circ g) = H(f) \circ H(g)$ et que $H(Id_E) = Id_{E'}$. On s'intéresse maintenant particulièrement à ces morphismes induits sur les homologies d'un complexe. Il se peut par exemple que deux morphismes de complexes distincts induisent les même morphismes d'homologie. La notion introduite ci-dessous donne un critère pour que ce soit le cas.

Définition 2.7. *Soit (E, d) et (E', d') deux complexes, et $f, g : E \to E'$ deux morphismes de complexes. On dit que f et g sont* homotopes *quand il existe une famille d'applications $h_n : E^n \to E'^{n-1}$ telle que*

$$f_n - g_n = d'^{n-1} \circ h_n + h_{n+1} \circ d^n$$

Proposition 2.1. *Si $f, g : (E, d) \to (E', d')$ sont deux morphismes de complexes homotopes, alors ils induisent les même morphismes d'homologie. C'est à dire pour tout $n \in \mathbb{Z}$ on a $H(f_n) = H(g_n)$.*

Démonstration. Pour tout entier n on a donc l'existence de $h_n : E^n \to E'^{n-1}$ tel que $f_n - g_n = d'^{n-1} \circ h_n + h_{n+1} \circ d^n$. On sait que $h_{n+1} \circ d^n$ est le morphisme nul sur $Z^n(E)$. De plus $Im(d'^{n-1} \circ h_n) \subset B^n(E')$. Ainsi $H(f_n - g_n) : H^n(E) \to H^n(E')$ est le morphisme nul. Donc $H(f_n) = H(g_n)$. □

Attardons nous maintenant sur la notion d'exactitude.

Définition 2.8. *Un complexe (A^n, d^n) est dit exact si :*

$$\forall n \in \mathbb{Z} \quad Im(d^n) = Ker(d^{n+1})$$

Nous allons voir maintenant que le fait qu'un triplé de complexe forme une suite exacte de complexe est quelque choses de "rigide", au sens où si une propriété est vrai pour deux facteurs cela peux entraîner que le dernier facteur la vérifie également. Donnons immédiatement un exemple utile pour la suite :

Proposition 2.2. *Si l'on a une suite exacte de complexe de chaîne dans* $\boldsymbol{Mod}_G$ *:*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

et que l'on suppose que A *et* B *sont des complexes exacts, alors* C *est un complexe exact.*

Démonstration. Soit $n \in \mathbb{Z}$. On considère le diagramme commutatif suivant donné par hypothèse, où les lignes sont exactes et le deux premières colonnes également.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_{n-1} & \xrightarrow{f_{n-1}} & B_{n-1} & \xrightarrow{g_{n-1}} & C_{n-1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle a_{n-1}} & & \downarrow{\scriptstyle b_{n-1}} & & \downarrow{\scriptstyle c_{n-1}} & & \\
0 & \longrightarrow & A_n & \xrightarrow{f_n} & B_n & \xrightarrow{g_n} & C_n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle a_n} & & \downarrow{\scriptstyle b_n} & & \downarrow{\scriptstyle c_n} & & \\
0 & \longrightarrow & A_{n+1} & \xrightarrow{f_{n+1}} & B_{n+1} & \xrightarrow{g_{n+1}} & C_{n+1} & \longrightarrow & 0
\end{array}$$

On sait que l'on a toujours $Im(c_{n-1}) \subset Ker(c_n)$ par définition d'un complexe de chaîne. Il faut donc établir l'inclusion réciproque.

Soit $y \in Ker(c_n)$. Par surjectivité de g_n il existe $x \in B_n$ tel que $g_n(x) = y$. Ainsi $c_n \circ g_n(x) = c_n(y) = 0$. Par commutativité du diagramme bas-droite, cela donne $g_{n+1} \circ b_n(x) = 0$. Ainsi

$$b_n(x) \in Ker(g_{n+1}) = Im(f_{n+1})$$

Il existe donc un $z \in A_{n+1}$ tel que $b_n(x) = f_{n+1}(z)$. Or

$$\begin{aligned}
f_{n+2} \circ a_{n+1}(z) =& b_{n+1} \circ f_{n+1}(z) \\
=& b_{n+1} \circ b_n(x) \\
=& 0
\end{aligned}$$

Cependant f_{n+1} est injective, d'où $a_{n+1}(z) = 0$ et $z \in Ker(a_{n+1}) = Im(a_n)$.

Il existe donc un $z_0 \in A_n$ tel que $a_n(z_0) = z$. Ainsi :

$$\begin{aligned}
b_n(x) =& f_{n+1}(z) \\
=& f_{n+1} \circ a_n(z_0) \\
=& b_n \circ f_n(z_0)
\end{aligned}$$

Et ainsi comme on travail dans une catégorie abélienne, $x - f_n(z_0) \in Ker(b_n) = Im(b_{n-1})$.

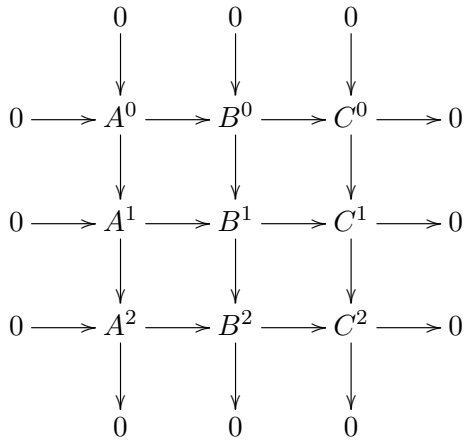
Il existe donc un $z_1 \in B_{n-1}$ tel que $b_{n-1}(z_1) = x - f_n(z_0)$. On applique alors g_n et il vient :

$$\begin{aligned}
g_n \circ b_{n-1}(z_1) &= g_n(x) - g_n \circ f_n(z_0) \\
c_{n-1} \circ g_{n-1}(z_1) &= y - 0
\end{aligned}$$

D'où $y \in Im(c_{n-1})$. □

On en déduit un corollaire bien utile :

Exemple 3. Si on a un diagramme commutatif :



On suppose que les colonnes sont exactes, et que les deux lignes du hauts sont exactes. Alors la ligne du bas est exacte. Notons les flèches $f_i : A^i \to B^i$ et $g_i : B^i \to C^i$, pour $i \in \{0, 1, 2\}$, et $x_i : X^i \to X^{i+1}$ pour $i \in \{0, 1\}$ et $X \in \{A, B, C\}$.

D'une part la ligne du bas est bien un complexe, en effet si $y \in Im(f_2)$, alors il existe $x_2 \in A^2$ tel que $f_2(x_2) = y$. Par surjectivité, il existe $x_1 \in A^1$ tel que $a_1(x_1) = x_2$. Donc on a

$$\begin{aligned} y &= f_2 \circ a_1(x_1) \\ &= b_1 \circ f_1(x_1) \end{aligned}$$

Et donc

$$\begin{aligned} g_2(y) &= g_2 \circ b_1 \circ f_1(x_1)) \\ &= c_1 \circ g_1 \circ f_1(x_1) \\ &= c_1(0) \\ &= 0 \end{aligned}$$

Ainsi on a bien $Im(f_2) \subset Ker(g_2)$.

Ainsi on a une suite exacte de complexes : (en regardant la "transposée" du diagramme ci-dessus)

$$0 \to X^0 \to X^1 \to X^2 \to 0 \ \ avec \ \ X^i = \{0 \to A^i \to B^i \to C^i \to 0\}$$

Car les colonnes du premier diagramme sont supposées exactes.

D'autre part, on a aussi supposé que les deux premières lignes du premier diagramme sont exactes, ce qui revient à dire que les X^0 et X^1 sont des complexes exacts. Ainsi on applique la proposition précédente (2.2), pour voir que X^2 est exacte, ce qu'il fallait démontrer.

2.3 Résolutions injectives

Nous allons maintenant nous attarder sur des notions qui permettrons la construction des foncteurs dérivés. On se place dans $\mathscr{C}$ une catégorie abélienne.

Définition 2.9. *Un objet I de $\mathscr{C}$ est dit* injectif *quand pour tout monomorphisme $f : A \to B$ et morphisme $\alpha : A \to I$ il existe $\beta : B \to I$ tel que $\alpha = \beta \circ f$, en terme de diagramme commutatif on a :*

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B \\ & & \downarrow{\scriptstyle \alpha} & \swarrow{\scriptstyle \beta} & \\ & & I & & \end{array}$$

Intuitivement, cela signifie que l'on peut toujours prolonger correctement les morphismes à valeur dans I.

Définition 2.10. *On dit qu'un catégorie abélienne $\mathscr{C}$ possède* suffisament d'injectif, *quand pour tout objet A de $\mathscr{C}$ il existe un monomorphisme $0 \to A \to I$ où I est un objet injectif.*

Définition 2.11. *Pour un objet M dans $\mathscr{C}$, on appelle* résolution injective *une suite exacte de la forme :*

$$0 \to M \to I^0 \to I^2 \to I^2 \to \dots$$

Où chaque I^n est un objet injectif de $\mathscr{C}$.

Proposition 2.3. *Si $\mathscr{C}$ possède suffisamment d'injectifs, alors tout objet admet une résolution injective.*

Démonstration. Soit un objet M, par hypothèse il existe I^0 tel qu'on ai un monomorphisme :

$$0 \longrightarrow M \xrightarrow{f_0} I^0$$

On note M^0 l'image de ce monomorphisme, et on peut alors construire de nouveau un monomorphisme : $0 \longrightarrow I^0/M^0 \xrightarrow{f_1'} I^1$ avec I^1 injectif. On peut alors construire le morphisme $f_1 : I^0 \to I^1$ composé de $I^0 \to I^0/M^0$ et $f^{1\prime}$.Le noyau du premier est M_0 et le second est un monomorphisme, donc le noyau de f_1 est bien $Im(f_0)$. On a donc la suite exacte :

$$0 \longrightarrow M \xrightarrow{f_0} I^0 \xrightarrow{f_1} I^1$$

En itérant ce processus on obtient la résolution voulue. □

Comme le choix des objets I^n n'est pas constructif, il n'y a pas de raison a priori que l'on puisse parler de **la** résolution injective d'un objet. La proposition suivante va nous servir à montrer que ce n'est pas un problème si insurmontable.

Proposition 2.4. *Soit M et M' deux objets de $\mathscr{C}$, et $\phi : M \to M'$. On suppose que l'on a une résolution injective $(I^n)_{n\in\mathbb{N}}$ de M' et une suite exacte E où $E^{-1} = M$ et $E^{-n} = 0$ pour $n \geq 2$.*

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & M & \longrightarrow & E^0 & \longrightarrow & E^1 & \longrightarrow & E^2 & \longrightarrow & \dots \\ & & \downarrow{\scriptstyle \phi} & & & & & & & & \\ 0 & \longrightarrow & M' & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & I^2 & \longrightarrow & \dots \end{array}$$

Alors il existe un $f = (f_i)_i$ un morphisme de complexe entre ces derniers tels que $\phi = f_{-1}$. De plus (et surtout !) deux tels morphismes sont homotopes.

Démonstration. Commençons par la construction du morphisme f cherché. On procède par récurrence sur $n \in \mathbb{N} \bigcup \{-1\}$. On initialise en posant $f_{-1} = \phi$. Supposons maintenant avoir construit $f_{-1}, f_0, ...f_n$. On a le diagramme commutatif suivant :

$$\begin{array}{ccccc} E^{n-1} & \xrightarrow{d_{n-1}} & E^n & \xrightarrow{d_n} & E^{n+1} \\ \downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle f_n} & & \\ I_{n-1} & \xrightarrow[i_{n-1}]{} & I_n & \xrightarrow[i_n]{} & I_{i_{n+1}} \end{array}$$

On a déjà vu que comme le premier carré est commutatif on a le morphisme induit :

$$f'_n : E_n/Im(d_{n-1}) \to I_n/Im(i_{n-1}).$$

En outre on a $\overline{d_n}$ et $\overline{i_{n+1}}$ les deux isomorphismes définis comme suis :

$$\begin{array}{ccc} E_n & \xrightarrow{d_n} & Im(d_n) \\ {\scriptstyle \pi_d}\downarrow & \nearrow_{\overline{d_n}} & \\ E_n/Ker(d_n) & & \end{array} \qquad et \qquad \begin{array}{ccc} I_n & \xrightarrow{i_n} & Im(i_n) \\ {\scriptstyle \pi_i}\downarrow & \nearrow_{\overline{i_n}} & \\ I_n/Ker(i_n) & & \end{array}$$

Or on a par exactitude des deux suite, $Im(d_{n-1}) = Ker(d_n)$ et $Im(i_{n-1}) = Ker(i_n)$, donc on a les égalités :

$$E_n/Ker(d_n) = E_n/Im(d_{n-1}) \qquad et \qquad I_n/Ker(i_n) = I_n/Im(i_{n-1})$$

Ainsi on a le diagramme suivant :

$$\begin{array}{ccccc} 0 & \longrightarrow & E_n/Ker(d_n) & \xrightarrow{\overline{d_n}} & E_{n+1} \\ & & \| & & \\ & & E_n/Im(d_{n-1}) & & \\ & & \downarrow{\scriptstyle f'_n} & & \\ & & I_n/Im(i_{n-1}) & & \\ & & \| & & \\ & & I_n/Ker(i_n) & & \\ & & \downarrow{\scriptstyle \overline{i_n}} & & \\ & & I_{n+1} & & \end{array}$$

Maintenant par injectivité de I_{n+1} on a une application $f_{n+1} : E_{n+1} \to I_{n+1}$ telle que :

$$f_{n+1} \circ \overline{d_n} = \overline{i_n} \circ f'_n$$

On y est presque, il suffit maintenant de vérifier que $f_{n+1} \circ d_n = i_n \circ f_n$. Or on a d'une part :

$$\begin{aligned} f_{n+1} \circ d_n &= f_{n+1} \circ \overline{d_n} \circ \pi_d \\ &= \overline{i_n} \circ f'_n \circ \pi_d \end{aligned}$$

Et d'autre part :

$$i_n \circ f_n = \overline{i_n} \circ \pi_i \circ f_n$$

Ainsi comme par construction de f'_n on a $f'_n \circ \pi_d = \pi_i \circ f_n$ en composant par $\overline{i_n}$ on a le résultat. Ainsi on a construit f_n pour tout $n \geq -1$, et $f_{-1} = \phi$.

Il reste à montrer que deux tels morphisme, disons f et g, sont homotopes. Nous allons procèder par récurrence sur n pour construire notre morphisme $h_n : E^n \to I^{n-1}$. En premier lieu on remarque qu'il suffit de poser $h_0 : E^0 \to M'$ comme étant le morphisme nul. En effet comme $f_{-1} = g_{-1} = \phi$ la condition d'homotopie est trivialement vérifiée.

Supposons avoir construit $h_0, \ldots, h_n$ tel que $f_{n-1} - g_{n-1} = i^{n-2} \circ h_{n-1} + h_n \circ d^{n-1}$. Montrons dans un premier temps que

$$f_n - g_n - i^{n-1} \circ h_n \text{ s'annule sur } Im(d^{n-1}).$$

On effectue le calcul suivant :

$$\begin{aligned}
(f_n - g_n - i^{n-1} \circ h_n) \circ d^{n-1} &= (f_n - g_n) \circ d^{n-1} - i^{n-1} \circ h_n \circ d^{n-1} \\
&= (f_n - g_n) \circ d^{n-1} - i^{n-1} \circ (f_{n-1} - g_{n-1} - i^{n-2} \circ h_{n-1}) \\
&= (f_n - g_n) \circ d^{n-1} - i^{n-1} \circ (f_{n-1} - g_{n-1}) \qquad \text{car } i \circ i = 0 \\
&= 0 \quad \text{car } f - g \text{ est un morphisme de complexe}
\end{aligned}$$

Pour simplifier les notations on pose $\alpha_n = f_n - g_n - i^{n-1} \circ h_n$. Ainsi on a $Im(d^{n-1}) \subset Ker(\alpha_n)$ et donc on peut construire le diagramme suivant :

$$\begin{array}{ccccc}
0 & \longrightarrow & E^n/Im(d^{n-1}) & \xrightarrow{\overline{d^n}} & E^{n+1} \\
 & & \downarrow{\scriptstyle \overline{\alpha_n}} & & \\
 & & I^n & &
\end{array}$$

Où les $\overline{\alpha_n}$ et $\overline{d^n}$ sont obtenus par passage au quotient (que l'on vient de justifier pour α_n, et qui est trivial pour d^n). Par injectivité de I^n on construit $h_{n+1} : E^{n+1} \to I^n$ faisant commuter le diagramme précédent. Il reste alors à vérifier que :

$$f_n - g_n = i^{n-1} \circ h_n + h_{n+1} \circ d^n$$

C'est à dire que :

$$\alpha_n = h_{n+1} \circ d^n$$

Si on note $\pi : E^n \to E^n/Im(d^{n-1})$ la surjection canonique, on a par construction :

$$\begin{aligned}
\alpha_n &= \overline{\alpha_n} \circ \pi \\
&= h_{n+1} \circ \overline{d_n} \circ \pi \\
&= h_{n+1} \circ d_n
\end{aligned}$$

Ainsi on a prouvé l'hérédité. La conclusion s'en suit.

□

2.4 Construction du δ-morphisme

Dans cette section nous développons l'arsenal nécessaire à la construction du foncteur dérivé. On reste bien entendu dans la catégorie A-**mod**, quitte à l'étendre grâce au théorème de Freyd-Mitchell. Nous commençons par une petite propriété, qu'il est bien utile d'avoir en tête.

Proposition 2.5. *Si (E, d) est un complexe, pour $n \geq 0$ on a la suite exacte :*

$$0 \to H^n(E) \to Coker(d^n) \to Ker(d^{n+2}) \to H^{n+1}(E) \to 0$$

Démonstration. Fixons $n \in \mathbb{N}$ et notons $d^{n+1} : E^{n+1} \to E^{n+2}$. On a déjà vu que d^{n+1} induit par passage au quotient un morphisme : $E^{n+1}/B^n \to B^{n+1}$. On a également $B^{n+1} \subset Z^{n+1} = Ker(d^{n+2})$. On a donc construit :

$$0 \longrightarrow Ker(d^{n+1})/Im(d^n) \xrightarrow{i} E^{n+1}/Im(d^n) \xrightarrow{d^{n+1}} Ker(d^{n+2}) \xrightarrow{p} Ker(d^{n+2})/Im(d^{n+1}) \longrightarrow 0$$

Et il suffit de vérifier que cette suite est exacte "au milieu", car la première flèche est injective vu comme une inclusion, et la dernière est surjective vu comme un passage au quotient. Ce qui est trivial par définition des ensembles en jeu. On reconnaît alors la suite exacte de la proposition, ce qui permet de conclure. □

On va maintenant utiliser le lemme du serpent pour construire un morphisme qui sera fondamental pour donner quelques bonnes propriétés du foncteur dérivé.

Théorème 2.3. *Si on a une suite exacte* de complexe

$$0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$$

Alors il existe une famille de morphismes naturels

$$\delta^n : H^n(G) \to H^{n+1}(E)$$

induisant une suite exacte longue :

$$\ldots \longrightarrow H^n(E) \xrightarrow{H^n(f)} H^n(F) \xrightarrow{H^n(g)} H^n(G) \xrightarrow{\delta^n} H^{n+1}(E) \xrightarrow{H^{n+1}(f)} \ldots$$

Démonstration. Fixons $n \in \mathbb{N}$. Le fait que la suite $E,\ F,\ G$ soit exacte impliquent respectivement que les 2^{ieme} et 3^{ieme} lignes du diagramme commutatif suivant sont exactes.

$$\begin{array}{ccccccc}
 & & H^n(E) & \longrightarrow & H^n(F) & \longrightarrow & H^n(G) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & Coker(d_E^n) & \longrightarrow & Coker(d_F^n) & \longrightarrow & Coker(d_G^n) \longrightarrow 0 \\
 & & \downarrow{\scriptstyle d'^{n+1}_E} & & \downarrow{\scriptstyle d'^{n+1}_F} & & \downarrow{\scriptstyle d'^{n+1}_G} \\
0 & \longrightarrow & Ker(d_E^{n+2}) & \longrightarrow & Ker(d_F^{n+2}) & \longrightarrow & Ker(d_G^{n+2}) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & H^{n+1}(E) & \longrightarrow & H^{n+1}(F) & \longrightarrow & H^{n+1}(G)
\end{array}$$

La proposition précédente nous assure que pour X un complexe concerné, $H^n(X) = Ker(d'^{n+1}_X)$ et $H^{n+1}(X) = Coker(d'^{n+1}_X)$. On conclu par application du lemme du serpent, et par "recollement" des suites exactes courtes ainsi créées. □

2.5 Foncteurs dérivés

Passons maintenant à la construction tant attendu des foncteurs dérivés. On se place dans une catégorie abélienne $\mathscr{C}$, qui possède suffisamment d'injectifs. On se donne un objet M de $\mathscr{C}$ ainsi qu'un foncteur F exact à gauche et additif de $\mathscr{C}$ dans une catégorie $\mathscr{B}$.

On se donne une résolution injective de M :

$$0 \to M \to I^0 \to I^1 \to I^2 \to \dots$$

Le foncteur F étant exact à gauche, on obtient un complexe de chaîne (**attention** ce n'est **pas** une suite exacte) :

$$0 \to F(M) \to F(I^0) \to F(I^1) \to F(I^2) \to \dots$$

Ce qui donne lieu aux groupes d'homologie : $H^n(F(I))$. C'est alors la propriété suivante qui permet de définir proprement le foncteur dérivé droit de F :

Proposition 2.6. *Si on se donne deux résolutions injectives* $0 \to M \to I^0 \to I^1 \to I^2 \to \dots$ *et* $0 \to M \to E^0 \to E^1 \to E^2 \to \dots$, *alors pour tout* $n \in \mathbb{N}$ *on a un isomorphisme entre* $H^n(F(I))$ *et* $H^n(F(E))$

Autrement dit, deux résolutions injectives donnent lieu à la même homologie.

Démonstration. On a le diagramme suivant, avec $\phi = Id_M$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & E^0 & \longrightarrow & E^1 & \longrightarrow & E^2 & \longrightarrow \dots \\ & & \downarrow{\scriptstyle \phi} & & & & & & & \\ 0 & \longrightarrow & M & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & I^2 & \longrightarrow \dots \end{array}$$

Par la proposition (2.4) on a un morphisme de complexe $(f_i : E^i \to I^i)_{i\in\mathbb{N}}$ avec $f_{-1} = Id_M$ entre ces deux résolutions injectives (il s'agit bien de suites exactes). On a de même $(g_i : I^i \to E^i)_i$ morphisme de complexe avec $g_{-1} = Id_M$.

En appliquant F au premier diagramme avec les $(f_i)_i$ on obtient :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F(M) & \longrightarrow & F(E^0) & \longrightarrow & F(E^1) & \longrightarrow & F(E^2) & \longrightarrow \dots \\ & & \downarrow{\scriptstyle F(\phi)=Id_{F(M)}} & & \downarrow{\scriptstyle F(f_0)} & & \downarrow{\scriptstyle F(f_1)} & & \downarrow{\scriptstyle F(f_2)} & \\ 0 & \longrightarrow & F(M) & \longrightarrow & F(I^0) & \longrightarrow & F(I^1) & \longrightarrow & F(I^2) & \longrightarrow \dots \end{array}$$

Et de même avec les $(g_i)_i$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F(M) & \longrightarrow & F(E^0) & \longrightarrow & F(E^1) & \longrightarrow & F(E^2) & \longrightarrow \dots \\ & & \uparrow{\scriptstyle F(\phi)=Id_{F(M)}} & & \uparrow{\scriptstyle F(g_0)} & & \uparrow{\scriptstyle F(g_1)} & & \uparrow{\scriptstyle F(g_2)} & \\ 0 & \longrightarrow & F(M) & \longrightarrow & F(I^0) & \longrightarrow & F(I^1) & \longrightarrow & F(I^2) & \longrightarrow \dots \end{array}$$

Alors les $(F(g_i) \circ F(f_i))_i$ et $Id_{F(E^i)}$ sont deux morphismes pour le diagramme :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F(M) & \longrightarrow & F(E^0) & \longrightarrow & F(E^1) & \longrightarrow & F(E^2) & \longrightarrow \dots \\ & & \downarrow{\scriptstyle Id_{F(M}} & & & & & & & \\ 0 & \longrightarrow & F(M) & \longrightarrow & F(E^0) & \longrightarrow & F(E^1) & \longrightarrow & F(E^2) & \longrightarrow \dots \end{array}$$

et donc $(F(g_i) \circ F(f_i))_i$ et $Id_{F(E^i)}$ sont homotopes, toujours par la proposition (2.4), et donc induisent les même homologies, c'est à dire :

$$H^n(F(f) \circ F(g)) = H^n(Id_{F(E)}) \qquad \text{pour tout } n \in \mathbb{N}$$

Or on sait que $H^n(F(f) \circ F(g)) = H^n(F(f)) \circ H^n(F(g))$ et d'autre part $H^n(Id_{F(E)})$ correspond évidement à l'identité sur $H^n(F(E))$. Ainsi :

$$H^n(F(f)) \circ H^n(F(g)) = Id_{H^n(F(E))}$$

On montre de la même façon que

$$H^n(F(g)) \circ H^n(F(f)) = Id_{H^n(F(I))}$$

Et ainsi que pour tout $n \in \mathbb{N}$, $H^n(F(f))$ et $H^n(F(g))$ sont des isomorphismes réciproques l'un de l'autre, et que donc $H^n(F(I))$ et $H^n(F(E))$ sont isomorphes. □

On peut alors sans équivoque donner la définition suivante :

Définition 2.12. *Avec les notations ci-dessus, on appelle* n^{ieme} foncteur dérivé droit *de F à l'objet M le groupe de cohomologie :*

$$R^nF(M) = H^nF(I)$$

qui est bien unique à isomorphisme près. On appellera foncteur dérivé droit *de F à l'objet M la famille* $(R^nF(M))_n$

Nous passons maintenant aux propriétés fondamentales que possède la familles des foncteurs dérivés. Dans la littérature on appelle un *δ-foncteur*, toute famille vérifiant ces propriétés.

Théorème 2.4. *Nous gardons les notations et hypothèses du début de paragraphe.*

i) *Pour tout $n \geq 0$ le n^{ieme} foncteur dérivé droit R^nF est un foncteur additif, bien définie à isomorphisme prêt*

ii) *On a une correspondance naturelle entre F et R^0F*

iii) *Pour toute suite exacte $0 \to M' \to M \to M'' \to 0$ et tout $n \geq 0$ on a l'existence d'un morphisme naturel :*

$$\delta^n : R^nF(M'') \to R^{n+1}F(M)$$

qui induit une suite exacte :

$$\cdots \to R^nF(M') \to R^nF(M) \to R^nF(M'') \to R^{n+1}F(M') \to \dots$$

iv) *Si on se donne un morphisme de suites exactes courtes entre :*

$$0 \to A' \to A \to A'' \to 0$$
$$et$$
$$0 \to B' \to B \to B'' \to 0$$

Alors pour tout $n \in \mathbb{N}$ on a les diagrammes commutatifs suivants :

$$\begin{array}{ccc} R^nF(A'') & \xrightarrow{\delta^n} & R^{n+1}F(A') \\ \downarrow & & \downarrow \\ R^nF(B'') & \xrightarrow{\delta^n} & R^{n+1}F(B') \end{array}$$

Démonstration. Par ce qui précède, on a bien **i)**. En outre **ii)** est clair car

$$R^0F(M) = Ker\left(F(I^0) \to F(I^1)\right) = F(M)$$

car F est exact à gauche. On admet **iv)** pour le moment. Il reste à prouver **iii)**.

Toute la démonstration réside dans la construction de la famille de morphismes δ^n. En premier lieu on considère I'^0 et I''^0 deux injectifs tels que :

$$\begin{array}{ccccccccc} & & 0 & & 0 & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & & & \downarrow & & \\ & & I'^0 & & \text{"?"} & & I''^0 & & \end{array}$$

On souhaite alors compléter ce diagramme en une suite exacte de complexes, pour y appliquer (2.3). Cela passe par la construction d'un objet à la place "?" et des morphismes donnant lieu à des suites exactes horizontales et verticales. Posons alors $I^0 = I'^0 \bigoplus I''^0$, qui à tout pour être un bon candidat horizontalement. On sait que I^0 est un objet injectif, en tant que somme directe d'objets injectifs. Construisons un monomorphisme $M \to I^0$.

D'une part, par injectivité de I'^0 et inclusion de M' dans I'^0, on peut prolonger le monomorphisme $M' \to I'^0$ en un monomorphisme $i_1 : M \to I'^0$. On pose d'autre part $i_2 : M \to M'' \to I''^0$. Le morphisme vertical cherché est alors :

$$f : \left\{ \begin{array}{ccc} M & \to & I'^0 \bigoplus I''^0 \\ m & \mapsto & i_1(m) + i_2(m) \end{array} \right. .$$

f est un monomorphisme car i_1 en est un, et que i_2 est un morphisme. On a alors construit le diagramme exact suivant, avec N', N et N'' les conoyaux correspondant

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I'^0 & \longrightarrow & I^0 & \longrightarrow & I''^0 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

L'exactitude de la troisième ligne découle immédiatement de la proposition (2.2) et de sont corollaire. On peut alors effectuer la même construction à partir de la suite des "N", et par induction on obtient :

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I'_{M'} & \longrightarrow & I_M & \longrightarrow & I''_{M''} & \longrightarrow & 0 \end{array}$$

Où les $I' : 0 \to X' \to I'_{X'}$ sont des résolutions injectives des objets correspondants, et telles que les lignes soient exactes. On applique alors le foncteur F à ce diagramme afin d'obtenir :

$$0 \to F(I') \to F(I) \to F(I'') \to 0$$

qui est exacte car $I = I' \bigoplus I''$ et F est exact à gauche. On applique alors le théorème (2.3) qui nous donne exactement la famille de morphismes voulue ! □

On remarque que si I est un objet injectif, ses foncteurs dérivés se simplifient :

Proposition 2.7. *Si I est injectif, alors pour $n > 0$ on a $R^n F(I) = 0$*

Démonstration. Cela découle simplement du fait que I admet la résolution injective $0 \to I \to I \to 0$. □

On va maintenant donner un théorème de prolongement de famille de foncteurs. De manière très générale, ce dernier serait vrai pour toute transformation naturelle entre un δ-foncteur et le foncteur dérivé, mais nous nous limiterons au cas des foncteurs dérivés. On raconte en fait que le foncteur dérivé est un δ-foncteur *universel*.

Théorème 2.5. *Soit $(R^i F)_{i\geq 0}$ et $(R^i G)_{i\geq 0}$ deux foncteurs dérivés, tel qu'on ai une transformation naturelle :*

$$f^0 : R^0 F = F \to R^0 G = G$$

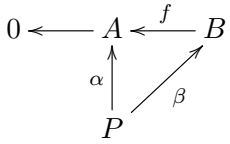
Alors il existe une unique famille $(f^n)_n$ de transformations naturelles prolongeant f^0 et commuttant avec les δ^n.

Démonstration. On trouvera une démonstration dans [Wei] page 47, dans le cas du foncteur dérivé gauche. □

2.6 Version duale du foncteur dérivé droit

Dans ce projet nous avons préféré mettre l'accès sur la cohomologie, plutôt que sur sa version duale l'homologie. Bien que cela soit naturel car nous verrons que le groupe de Brauer se construit comme un groupe cohomologique, il est sain de regarder ce qu'il se passe en homologie. En effet, outre la pure curiosité, il est en général plus facile de construire des objets que l'on appelle *projectifs*, qui sont les duaux des objets injectifs. Nous renvoyons à l'oeuvre de Weibel : *An introduction to homological algebra*[Wei] pour les démonstrations. On se place dans une catégorie abélienne $\mathscr{C}$.

Définition 2.13. *Soit P un objet de $\mathscr{C}$ est dit* projectif *quand pour tout épimorphisme $f : A \to B$ et morphisme $\alpha : P \to B$, il existe $\beta : P \to B$ tel que $\alpha = f \circ \beta$.*



On voit qu'il s'agit bien de la notion duale d'objet *injectif* car il s'agit exactement des objets injectifs de $\mathscr{C}^{op}$ (on a juste "renverser" les flèches). On peut alors également parler de résolutions projectives :

Définition 2.14. *Une* résolution projective *d'un objet M est un complexe $(P_i)_i$:*

$$\ldots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

qui est exact et où tous les P_i sont des objets projectifs.

Comme dans le cas injectif, si pour tout objet A de $\mathscr{C}$ on a une surjection $P \to A$ avec P projectif, alors tout objet A admet une résolution projective. On exprime bien sûr l'hypothèse précédente par $\mathscr{C}$ contient assez de projectifs. Et fort heureusement, comme dans le cas injectif, La catégorie R-**Mod** contient assez de projectifs.

Dans ce cas on peut encore démontrer que deux résolutions projectives d'un même objet donnent lieu aux mêmes groupes qualifiés cette fois de *groupes d'homologies*. La différence notable est que dans le cas cohomologique on a une suite "à droite" de M, et dans le cas homologique on a une suite "à gauche". On parle alors pour des foncteurs exacts à droite F, du *foncteur dérivé gauche* en l'objet A noté $L_iF(A)$, définit par les groupes d'homologie d'une résolution projective de A à laquelle on applique F.

Revenons à ce que l'on disait en début de paragraphe, pourquoi a-t-on plus facilement des objets projectifs qu'injectifs ? Cela découle de la propriété suivante :

Proposition 2.8. *Un module est projectif si et seulement si il est facteur direct d'un module libre.*

On trouve une démonstration de ce résultat dans *Algèbre, Chapitre 2* de Bourbaki, au paragraphe 2.

Cette vision *projective* nous est particulièrement utile dans le prochain paragraphe. Nous verrons que dans certains cas, cette vision projective explique l'annulation de groupes cohomologiques. Cela explique aussi la partie 3 de l'annexe, où pour calculer des H^2, nous passons par une résolution libre.

2.7 Cohomologie des groupes

2.7.1 Généralités et modules induits

On considère A un G-module. On note comme au théorème (2.2) A^G les invariant de A sous l'action de G. On a vu que le foncteur associé $F : A \mapsto A^G$ est additif, exact à gauche. Nous avons maintenant en main toutes les cartes pour donner la définition des groupes de cohomologie de G à valeur dans A.

Définition 2.15. *Cohomologie des groupes*
Pour $q \in \mathbb{N}$ on note $H^q(G, A) = R^qF(A)$ le q^{ieme} groupe de cohomologie de G à coefficient dans A

Par propriétés sur le foncteur dérivé on obtient les caractéristiques suivantes :

Proposition 2.9. *Avec les mêmes notations :*

- $H^0(G, A) = A^G$.
- *Si $q \geq 1$ et A est injectif, alors $H^q(G, A) = 0$.*

On va voir un exemple d'objet dont le $n - ieme$ groupe d'homologie s'annule pour $n \geq 1$. On note $\Gamma = \mathbb{Z}[G]$ l'algèbre du groupe G, qui est l'ensemble des sommes formelles presque nulles sur G.

Définition 2.16. *Induit d'un G-mudule*
Soit A un G-module, on appelle l'induit de A, l'objet $A^* = Hom_{\mathbb{Z}}(\Gamma, A)$.

Proposition 2.10. *Soit A un G-module, alors A^* est muni d'une structure de G-module, et A se plonge naturellement dans A^*.*

Démonstration. Pour la structure il suffit de poser :

$$g \in G \; f \in A^* \quad (g.f)(\sum_{s\in G} n_s s) = f(\sum_{s\in G} n_s sg)$$

Et on à le morphisme injectif $\phi : A \to A^*$ où pour $a \in A$:

$$\phi_a : \left\{ \begin{array}{rcl} \Gamma & \to & A \\ \sum_{s\in G} n_s s & \mapsto & \sum_{s\in G} n_s (s.a) \end{array} \right. .$$

Il est alors clair que si $\phi_a = \phi_b$, en évaluant en 1 on trouve $a = b$. D'où l'injectivité. Il est clair qu'il s'agit d'un morphisme de G-module. □

Proposition 2.11. *Soit A un groupe abélien. Pour B un G-module, on a l'identification :*

$$Hom_{\mathbb{Z}}(B, A) \cong Hom_G(B, A^*)$$

Démonstration. Donnons nous un élément $\psi \in Hom_{\mathbb{Z}}(B, A)$. Alors pour tout $b \in B$ on définit $\phi_b \in A^*$ par

$$\phi_b : \left\{ \begin{array}{ccc} \Gamma & \to & A \\ \sum_{s\in G} n_s s & \mapsto & \psi(\sum_{s\in G} n_s(s.b)) \end{array} \right. .$$

On vérifie immédiatement que ϕ_b est dans A^*, car ψ est dans $Hom_{\mathbb{Z}}(B, A)$. Soit maintenant $g \in G$ et $b \in B$. Alors

$$\begin{aligned} (g.\phi_b)(\sum_{s\in G} n_s s) =& \phi_b(\sum_{s\in G} n_s sg) \\ =& \psi(\sum_{s\in G} n_s(sg).b) \\ =& \psi\left(\sum_{s\in G} n_s(s.(g.b))\right) \\ =& \phi_{g.b}(\sum_{s\in G} n_s s) \end{aligned}$$

Ainsi l'application ϕ est dans $Hom_G(B, A^*)$. On considère alors

$$u : \left\{ \begin{array}{ccc} Hom_{\mathbb{Z}}(B, A) & \to & Hom_G(B, A^*) \\ \psi & \mapsto & \phi \end{array} \right. .$$

Montrons que u est injective. Si on a $\phi \in Ker(u)$ alors ϕ_b est l'application nulle pour tout b dans B. En particulier à b fixé :

$$\begin{aligned} 0 =& \phi_b(1) \\ =& \psi(b) \end{aligned}$$

Et donc ψ est nulle sur B. Il reste à voir que u est surjective. Prenons un $\theta \in Hom_G(B, A^*)$. Alors :

$$\begin{aligned} \theta(b)(\sum_{s\in G} n_s s) &= \left(\sum_{s\in G} n_s s.\theta(b)\right)(1) \quad \text{car } A^* \text{ est un } G\text{-module donc un } \Gamma\text{-module} \\ &= \theta(\sum_{s\in G} n_s s.b)(1) \quad \text{car } B \text{ est un } G\text{-module donc un } \Gamma\text{-module} \end{aligned}$$

Cela donne l'idée de définir :

$$\psi : \left\{ \begin{array}{ccc} B & \to & A \\ b & \mapsto & \phi(b)(1) \end{array} \right. .$$

Car le calcul précédent montre que si $\sum_{s\in G} n_s s = k.1$ pour n'importe quel $k \in \mathbb{Z}$, alors ψ est bien dans $Hom_{\mathbb{Z}}(B, A)$. En outre on a :

$$\forall g \in G\, b \in B \;\; u(\psi)(b)(g) = \psi(gb) = \theta(gb)(1) = \theta(b)(g)$$

Ainsi $u(\psi) = \theta$, et u est surjective.

□

Illustrons les propos du paragraphe précédent, dans lequel nous affirmions que la vision *projective* peut nous permettre de calculer des groupes.

Proposition 2.12. *Soit*

$$\cdots \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

une résolution projective de $\mathbb{Z}$. Si A est un G-module, le complexe

$$0 \to Hom_G(P_0, A^*) \to Hom_G(P_1, A^*) \to \dots$$

est exact.

Démonstration. Les P_i sont des $\mathbb{Z}[G]$-modules projectifs, donc des $\mathbb{Z}$-modules projectifs. Or $\mathbb{Z}$ est principal, donc les P_i sont en fait libre. Ainsi on a une suite exacte de modules libres, alors par la théorie des modules et du foncteur $Hom(., A)$, on a une suite qui reste exacte :

$$0 \to Hom_{\mathbb{Z}}(P_0, A) \to Hom_{\mathbb{Z}}(P_1, A) \to Hom_{\mathbb{Z}}(P_2, A) \to \dots$$

En outre on a vu que pour $i \geq 0$ $Hom_{\mathbb{Z}}(P_i, A) \cong Hom_G(P_i, A^*)$, donc on a la suite voulue. □

Ce qui nous amène au calcul des groupes de cohomologie $H^i(G, A)$, par celui d'un autre complexe :

Théorème 2.6. *Soit*

$$\cdots \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

une résolution projective de $\mathbb{Z}$, et A un G-module. Alors les $H^i(G, A)$ sont les groupes de cohomologie du complexe :

$$0 \to Hom_G(P_0, A) \to Hom_G(P_1, A) \to ....$$

Démonstration. Voir [Har], page 21. □

Ainsi en combinant les deux derniers résultats on obtient :

Proposition 2.13. *Soit A un G-module, alors*

$$\forall n \geq 1 \, H^n(G, A^*) = 0$$

2.7.2 Changements de groupes

On se demande maintenant comment se comportent ces objets si on change le groupe de base G. Considérons G' un autre groupe, ainsi que $f : G' \to G$ un morphisme. On peut alors munir A d'une structure de G'-module par :

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

On notera f^*A cette nouvelle structure sur A, sauf si aucune ambiguïté n'est possible.

Proposition 2.14. *Avec ces notations, A^G est un sous-groupe de $(f^*A)^{G'}$*

Démonstration. En effet, il suffit de voir que si $a \in A^G$, alors pour tout $s' \in G'$ on a :

$$s'.a = f(s').a = a$$

□

Ainsi cela nous donne par passage à l'homologie un morphisme de $H^0(G, A)$ dans $H^0(G', f^*A)$.

Proposition 2.15. *Pour chaque $n \geq 0$, le morphisme $f : G \to G'$ induit un morphisme :*

$$f_n^* : H^n(G, A) \to H^n(G', f^*A)$$

Démonstration. On a vu que f induisait un morphisme du foncteur $H^0(G, A)$ dans le foncteur $H^0(G', f^*A)$, or le foncteur dérivé est un δ-foncteur *universel* par le théorème (2.5). Ainsi on peut prolonger de manière unique notre première transformation naturelle, pour obtenir la famille voulue. □

On a vu comment obtenir une relation entre $H^n(G, A)$ et $H^n(G', A)$ si on a une relation entre G et G'. Attardons nous maintenant sur ce qu'il se passe si l'on change également le X-module A en question.

Définition 2.17. *applications compatibles*
Si on pose maintenant A' un autre G'-module, et $g : A \to A'$ une application additive. On dit que f et g sont compatibles *si :*

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

Dans toute la suite A' est un G'-module fixé. On remarque que le fait que g soit compatible avec f, coïncide entièrement avec le fait que g est un morphisme de G'-module de f^*A dans A'.

Proposition 2.16. *Avec les mêmes notations.*
Pour $n \in \mathbb{N}$, g induit un morphisme :

$$g_n^* : H^n(G', f^*A) \to H^q(G', A')$$

Démonstration. Par le même raisonnement que précédemment il suffit de voir que g induit un morphisme de $(f^*A)^{G'}$ sur $A'^{G'}$, que l'on prolongera par universalité du foncteur dérivé. Ce dernier fait découle du calcul suivant, pour $a \in (f^*A)^{G'}$ et $s' \in G'$:

$$\begin{aligned} s'.g(a) =& g(f(s').a) \quad \text{par compatibilité de } f \text{ et } g \\ =& g(s'.a) \quad \text{par définition de } f^*A \\ =& g(a) \quad \text{car } a \in (f^*A)^{G'} \end{aligned}$$

□

Définition 2.18. *On peut ainsi construire par composition le morphisme* associé *au couple (f, g) : (en conservant les hypothèses sur f et g)*

$$g_n^* \circ f_n^* := (g, f)_n^* : H^n(G, A) \to H^n(G', A')$$

Exemple 4. Si H est un sous-groupe de G et A un G-module, on peut prendre pour f l'injection $H \to G$, qui donne lieu aux morphismes dit de restriction :

$$Res^n : H^n(G, A) \to H^n(H, A)$$

Exemple 5. Si maintenant H est un sous-groupe *distingué* de G, alors A^H a une structure de G/H-module, les morphismes canoniques $\pi : G \to G/H$ et $i : A^H \to A$ sont compatibles, on obtient ainsi les morphismes *d'inflation* :

$$Inf^n : H^n(G/H, A^H) \to H^n(G, A)$$

En effet :

$$\forall a \in A^H \; \forall h \in H \; \forall g \in G \quad gh.a = g.(h.a) = g.a$$

d'où on peut voir A^H comme un G/H-module par : $\pi(g).a = g.a$. En outre pour $a \in A^H$ et $g \in G$:

$$\begin{aligned} i(\pi(g).a) &= \pi(g).a \quad \text{vu dans A} \\ &= g.a \quad \text{par définition de l'action} \\ &= g.i(a) \end{aligned}$$

D'où la compatibilité.

Avant de passer à la construction du groupe de Brauer à proprement dit, il nous reste un dernier résultat à donner, qui nous assurera la "bonne" définition du groupe en question.

Théorème 2.7. *Soit G un groupe, et $t \in G$. Pour tout G-module A, on considère les morphismes :*

$$f_t : \left\{ \begin{array}{ccc} G & \to & G \\ s & \mapsto & tst^{-1} \end{array} \right.$$

et

$$g_t : \left\{ \begin{array}{ccc} A & \to & A \\ a & \mapsto & t^{-1}.a \end{array} \right. .$$

Alors f_t et g_t sont compatibles, et le couple associé définit des automorphismes $g_t^* \circ f_t^* = \sigma_t^n(A)$ de $H^n(G, A)$, qui sont en fait égaux à l'identité.

Démonstration. Montrons dans un premier temps que f_t et g_t sont compatibles (on les notera f et g respectivement dans la fin de la preuve), ce qui découle aisément du calcul :

$$g(f(s).a) = t^{-1}.(tst^{-1}.a) = st^{-1}.a = s.(t^{-1}.a) = s.g(a)$$

Montrons maintenant que pour tout A, les $\sigma_t^n(A)$ induits sont l'identité. On procède par récurrence sur n. En premier lieu Si $n = 0$, alors pour tout objet A, $H^n(G, A) = A^G$, il est alors clair que la composée des morphismes est l'identité par invariance de A^G. Soit $n \in \mathbb{N}$ tel que pour tout objet B on a $\sigma_t^n(B) : H^n(G, B) \to H^n(G, B) = Id$. Soit A un G-module. On plonge A dans le module co-induit $A^* := Hom_{\mathbb{Z}}(Z[G], A)$, et on note $B = A^*/A$. On a alors la suite exacte :

$$0 \to A \to A^* \to B \to 0$$

Par la propriétés (2.4) **iii)** du foncteur dérivé cette suite exacte donne lieu à la suite exacte longue de cohomologie :

$$\ldots \longrightarrow H^n(G, A) \longrightarrow H^n(G, A^*) \longrightarrow H^n(G, B) \xrightarrow{\delta^n} H^{n+1}(G, A) \longrightarrow H^{n+1}(G, A^*) \longrightarrow \ldots$$

Or comme A^* est l'induit de A, on a pour $m \geq 1$, $H^m(G, A^*) = 0$ par la proposition (2.13). On a en particulier la surjection :

$$\delta^n : H^n(G, B) \to H^{n+1}(G, A)$$

car la suite précédente est exacte. Encore, la propriété (2.4) **iv)** du foncteur dérivé nous donne le diagramme commutatif suivant :

$$\begin{array}{ccc} H^n(G, B) & \xrightarrow{\delta^n} & H^{n+1}(G, A) \\ \downarrow{\scriptstyle \sigma_t^n(B)} & & \downarrow{\scriptstyle \sigma_t^{n+1}(A)} \\ H^n(G, B) & \xrightarrow[\delta^n]{} & H^{n+1}(G, A) \end{array}$$

Soit maintenant $y \in H^{n+1}(G, A)$. Par surjectivité il existe $x \in H^n(G, B)$ tel que $y = \delta^n(x)$. Alors la commutativité du diagramme ci-dessus donne :

$$\begin{aligned}\sigma_t^{n+1}(A)(y) =& \sigma_t^{n+1}(A) \circ \delta^n(x) \\ =& \delta^n(x) \circ \sigma_t^n(B)(x) \\ =& \delta^n(x) \\ =& y\end{aligned}$$

Ainsi $\sigma_t^{n+1}(A)$ est bien l'identité, ce qui conclu la récurence.

□

2.7.3 Groupe de Brauer d'un corps

Disclaimer Dans ce chapitre un corps sera toujours supposé commutatif, un corps non nécessairement commutatif sera appelé algèbre à division.

Nous allons enfin pouvoir passer à la définition du groupe de Brauer, d'un point de vue cohomologique.

Nous fixons k un corps, et K/k une extension galoisienne, de groupe de Galois G. Il est clair que G agit sur le groupe multiplicatif K^* de manière à lui donner une structure de G-module. Nous noterons alors dans ce cas :

$$H^q(K/k) = H^q(G, K^*)$$

On espère en réalité que ces derniers groupes ne dépendent pas de K, à isomorphisme près.

Proposition 2.17. *Si K et K' sont deux corps k-isomorphes, donnant lieux à des extensions galoisiennes de k, alors on a l'isomorphisme canonique*

$$H^n(K/k) \cong H^n(K'/k)$$

Démonstration. On note G (resp. G') le groupe de Galois de l'extension K (resp. K').On note $g : K^* \to K'^*$ l'isomorphisme. Ce dernier induit un morphisme de groupe $f : G' \to G$ qui à $s' \in G'$ associe $s = g^{-1} \circ s' \circ g$. Le calcul qui suit montre alors que f et g sont compatibles.

$$\begin{aligned}\text{pour } s' \in G' \; k \in K \quad g(f(s').k) &= g(f(s').k) \\ &= g(f(s')(k) \\ &= g\left(g^{-1}(s'(g(k)))\right) \\ &= s'(g(k)) \\ &= s'.g(k)\end{aligned}$$

On a alors des isomorphismes induits (ici $G = G'$) :

$$(g, f)_n^* : H^n(K/k) \to H^n(K'/k)$$

De plus ces morphismes sont indépendants de g (c'est pour cela que l'on parle d'isomorphisme canonique). En effet si on avait un autre isomorphisme $g' : K \to K'$, alors on aurait par la théorie de Galois un $t \in G$ tel que $g = g' \circ t$. Et donc pour $k \in K^*$ on a :

$$\begin{aligned}g(k) =& g'(t(a)) \\ =& g' \circ g_{t^{-1}}(a)\end{aligned}$$

Et donc comme g_0^* et $g_0'^* \circ g_{t^{-1}0}^*$ coïncident,on a par unicité du prolongement (théorème (2.5)) pour tout $n \in \mathbb{N}$:

$$g_n^* = g_n'^* \circ g_{t^{-1}n}^*$$

Comme précédemment on construit f et f', compatibles avec respectivement g et g'. Ainsi par définition on a pour $s' \in G'$:

$$\begin{aligned} f(s') &= g^{-1} \circ s' \circ g \\ &= t^{-1} \circ g'^{-1} \circ s' \circ g' \circ t \\ &= t^{-1} \circ f'(s') \circ t \\ &= f_{t^{-1}} \circ f'(s') \end{aligned}$$

Et donc comme f_0^* et $f_{t^{-1}0}^* \circ f_0'^*$ coïncident,on a par unicité du prolongement pour tout $n \in \mathbb{N}$:

$$f_n^* = f_{t^{-1}n}^* \circ f_n'^*$$

Donc on peut conclure par le théorème (2.6) appliqué à t^{-1} que :

$$g_n^* \circ f_n^* = g_n'^* \circ g_{t^{-1}n}^* \circ f_{t^{-1}n}^* \circ f_n'^* = g_n'^* \circ \sigma_{t^{-1}}^n(K) \circ f_n'^* = g_n'^* \circ f_n'^*$$

□

Proposition 2.18. *Si k^s une clôture séparable de k (unique à isomorphisme près), alors k^s/k est galoisienne.*

Démonstration. Comme l'extension est séparable et algébrique, il suffit de voir qu'elle est normale. Ce qui vient de la maximalité. □

On en vient enfin à la notion de groupe de Brauer de k ! On peut donc grâce à la propriété précédente, considérer le *le groupe de Galois absolu* de k, le groupe $G = Gal(k^s/k)$ agissant sur k^{s*}. La clôture séparable étant unique à isomorphisme près, nous avons vu plutôt que les $H^q(k^s/k)$ ne dépendent pas de k^s. Nous les noterons donc $H^q(\ /k)$.

Définition 2.19. *On définit le* groupe de Brauer *de k par :*

$$Br(k) = H^2(\ /k)$$

2.8 Théorème 90 de Hilbert

Nous allons démontrer ici un résultat crucial, qui sera utilisé deux fois pas la suite, lors de la dernière partie de ce projet.

Nous fixons dans ce paragraphe K/k une extension galoisienne finie. Comme vu précédemment, nous notons $G = Gal(K/k)$. Si $GL_n(K)$ est le groupe des matrices à coefficients dans K, on fait agir G sur le groupe linéaire coefficients par coefficients. On peut alors définir le groupe de cohomologie : $H^1(G, GL_n(K))$. L'objectif est alors de démontrer le théorème suivant :

Théorème 2.8. *(*90 de Hilbert*).* $H^1(G, GL_n(K))$ est réduit au neutre

Pour y parvenir, énonçons d'abord un résultat général sur l'indépendance des morphismes :

Proposition 2.19. *Soit $(M, *)$ un monoïde et K un corps. Alors toute famille de morphismes $(M, *) \to (K^*, \times)$ deux à deux distincts est libre dans le K-espace $\mathscr{F}(M, E)$*

Démonstration. Il suffit de traiter le cas des familles finies. Procédons par récurrence sur le cardinal de la famille $n \in \mathbb{N}^*$. Si $n = 1$ c'est clair, car 0_M est envoyé sur 1_K par tout morphisme.

Si on note $(\phi_i)_{i \leq n+1}$ la famille en question, et si on prend $\lambda_1, \ldots, \lambda_{n+1} \in K$ tels que :

$$\sum_{i=1}^{n+1} \lambda_i \phi_i = 0$$

Soit $x \in M$, alors pour tout $y \in M$ on a :

$$0 = \sum_{i=1}^{n+1} \lambda_i \phi_i(x * y) \tag{1}$$

$$= \sum_{i=1}^{n+1} \lambda_i \phi_i(x) \phi_i(y) \tag{2}$$

et

$$0 = \sum_{i=1}^{n+1} \lambda_i \phi_i(y) \tag{3}$$

Ainsi en faisant l'opération $(2) - \phi_{n+1}(x) \times (3)$, on élimine le dernier terme, on obtient donc :

$$\forall y \in M \quad \sum_{i=1}^{n} \lambda_i \phi_i(y) \left(\phi_i(x) - \phi_{n+1}(x)\right) = 0$$

Or par hypothèse de récurrence les $\phi_1, \ldots, \phi_n$ sont libres, on a donc pour $i \in [\![1, n]\!]$:

$$\lambda_i \left(\phi_i(x) - \phi_{n+1}(x)\right) = 0$$

Ceci étant vrai pour tout $x \in K$, et les ϕ_i étant deux à deux distincts on a pour tout $i \in [\![1, n]\!],\ \lambda_i = 0$. Ainsi il reste $\lambda_{n+1}\phi_{n+1} = 0$ qui implique $\lambda_{n+1} = 0$ comme dans le cas $n = 1$. □

Passons à la démonstration du théorème 90 de Hilbert.

Démonstration. (On considère admis les résultats sur le calcul cohomologique au moyen de cochaînes, *cf* la troisième partie de l'annexe) Soit $a : s \mapsto a_s$ un 1-cocycle, montrons que c'est également un cobord, c'est à dire qu'il existe $b \in GL_n(K)$ tel que :

$$\forall s \in G \quad a_s = s(b)b^{-1}$$

Soit $c \in M_n(K)$ quelconque, on pose : $b_0 = \sum_{t \in G} a_t t(c)$. On a pour tous $s \in G$:

$$\begin{aligned} s(b_0) &= \sum_{t \in G} s(a_t) st(c) \\ &= \sum_{t \in G} a_s^{-1} a_{st} st(c) \quad \text{car } a \text{ est un 1-cocycle} \\ &= a_s^{-1} b_0 \end{aligned}$$

Il suffit donc de bien choisir la matrice c, pour fair de b_0 un élément de $GL_n(K)$, pour l'inverser. Soit $x \in K^n$ fixé.

Notons $b(x) = \sum_{s \in G} a_s(s(x))$. Montrons que les $b(x)$ engendre K^n, par dualité. Si u est une forme linéaire nulle sur tous les $b(x)$, alors :

$$\forall k \in K \quad 0 = u(b(kx)) = \sum_{s \in G} a_s u(s(k)s(x)) = \sum_{s \in G} s(k) a_s u(s(x))$$

Ceci nous donne une relation linéaire sur les $s \in G$, en considérant la variable k. Or par la proposition précédente, ces derniers forment une famille libre, ainsi les $a_s u(s(x))$ sont tous nuls. Or les a_s sont inversibles par définition donc on a $\forall x \in K^n\ u(s(x)) = 0$, et donc $u = 0$.

On peut alors considérer $x_1, \dots, x_n$ dans K^n tels que les $b(x_i)$ soient K-indépendants. On prend alors pour c la matrice de l'application qui envoie la base canonique (e_i) de K^n sur la famille (x_i). Dans ce cas on a pour $i \in [\![1, n]\!]$:

$$\begin{aligned} b_0 e_i =& \sum_{t \in G} a_t t(c) e_i = \sum_{t \in G} a_t t(ce_i) \quad \text{car } e_i \text{ est à coefficients dans } k, \text{ donc invariant par } G \\ =& \sum_{t \in G} a_t t(x_i) \\ =& b(x_i) = y_i \end{aligned}$$

Ainsi b_0 envoie une base sur une base, elle est donc inversible, ce qu'il fallait démontrer.

□

3 Algèbre centrale simple sur un corps

Dans cette section on s'intéresse à des objets : les algèbres centrales simples dont un exemple crucial est l'algèbre des matrices carrées d'une taille donnée. On définira une relation d'équivalence sur ces algèbres et on pourra munir l'ensemble de ces algèbres modulo cette relation d'équivalence d'une structure de groupe...

3.1 Premières définitions, premiers exemples

Soit k un corps, toutes les k-algèbres considérées dans la suite sont supposées de dimension finie sur k.

Définition 3.1 (Algèbre simple)**.** *Une k-algèbre A est dite simple si son anneau sous-jacent est simple, c'est à dire qu'il ne possède pas d'idéal bilatère non trivial.*

Définition 3.2. *Soit A une k-algèbre, on appelle centre de A et on note $Z(A)$ l'ensemble $\{a \in A, \forall b \in A, ab = ba\}$, on a immédiatement : si A est une k-algèbre, $Z(A)$ est une extension de k.*

Définition 3.3 (Algèbre centrale)**.** *Une k-algèbre A est dite centrale si son centre est exactement k.*

Définition 3.4 (Module simple)**.** *Un module M sur un anneau A est dit simple si ses seuls sous-A-modules sont 0 et M.*

Définition 3.5 (algèbre opposée)**.** *Soit $(A, +, *, .)$ une k-algèbre, on note A^{OP} son algèbre opposée définie par $(A, +, *^{OP}, .)$ où pour $x, y \in A$, $x *^{OP} y = y * x$ c'est une algèbre ayant la même structure d'espace vectoriel sous-jacente que A mais dans laquelle on renverse le produit.*

Définition 3.6. *Si M est un A-module, on note $End_A(M)$ l'ensemble des endomorphismes A-linéaires de M.*

Exemple 1. Si D est une k-algèbre à division, c'est une k-algèbre simple.

Exemple 2. Soit $n \in \mathbb{N}^*$ et D une k-algèbre simple, l'algèbre $\mathscr{M}_n(D)$ est centrale sur $Z(D)$ et simple.

Démonstration. Si $n = 1$, le résultat est évident, supposons $n \geq 2$:
Soit A dans le centre de $\mathscr{M}_n(D)$, Soit $\mathscr{D}$ une droite de D^n, F un supplémentaire de $\mathscr{D}$ et P la matrice de la projection sur $\mathscr{D}$ parallèlement à F. A commute à P et $\mathscr{D}$ est stable par P, donc par A, donc tous les vecteurs de k^n sont vecteurs propres de A, A est donc une matrice scalaire. A commute en particulier avec les autres matrices scalaires, ce qui impose que ces éléments diagonaux commutent à tous les éléments de D. Donc $Z(\mathscr{M}_n(D) \cong Z(D)$.

Soit alors $M \in \mathscr{M}_n(k)$ non nulle, montrons que l'idéal bilatère $\mathscr{I}$ engendré par M est $\mathscr{M}_n(D)$:
Soient $i, j \in [\![1, n]\!]$ On pose $E_{i,j}$ la matrice ayant un 1 en place (i, j) et 0 ailleurs. les $(E_{i,j})_{i,j \in [\![1,n]\!]}$ engendrent $\mathscr{M}_n(D)$, il suffit donc de montrer que $\mathscr{I}$ les contient tous, de plus, la relation

$$E_{i,k}E_{k,l}E_{l,j} = E_{i,j} \text{ pour } i, j, k, l \in [\![1, n]\!]$$

montre qu'il suffit que $\mathscr{I}$ en contienne 1 pour tous les contenir.
De là, comme A est non nulle, il existe $i, j \in [\![1, n]\!]$ tels que $A_{i,j} \neq 0$ et par simplicité de D, $D = (A_{i,j})$ donc il existe $d_1, d_2 \in D$ tels que $d_1 A_{i,j} d_2 = 1$, on a :

$$(d_1 E_{i,i}) A (d_2 E_{j,j}) = E_{i,j} \in \mathscr{I},$$

donc $\mathscr{I} = \mathscr{M}_n(D)$
$\mathscr{M}_n(D)$ est bien une k-algèbre centrale sur $Z(D)$ simple.

□

3.2 Produit tensoriel de k-algèbres

Propriété-définition Soient E et F deux k-espaces vectoriels, il existe un k-espace vectoriel noté $E \otimes_k F$ et une application bilinéaire Φ vérifiant la propriété universelle suivante :

Quel que soit G un k-espace vectoriel, et φ une application bilinéaire de $E \times F \longrightarrow G$, il existe une unique application linéaire $f : E \otimes_k F \longrightarrow G$ telle que $\varphi = f \circ \Phi$

De plus un tel couple $(E \otimes_k F, \Phi)$ est unique à isomorphisme près. Pour $(x, y) \in E \times F$, on note $x \otimes_k y := \Phi(x, y)$
Enfin, si $(f_i)_{i\in I}$ est une base de F, et $(e_j)_{j\in J}$ est une base de E, alors $(e_i \otimes_k f_j)_{i\in I, j\in J}$ est une base de $E \otimes_k F$

Proposition 3.1. *Soient E et F des k-espaces vectoriels de dimension finie, et $(f_1, ..., f_r)$ une base de F, si $x \in E \otimes_k F$ alors il existe $(x_1, ..., x_r)$ des éléments de E tels que $x = \sum_{i=1}^{r} x_i \otimes_k f_i$, et cette écriture est unique.*

Démonstration. Ceci découle du fait que $(e_i \otimes_k f_j)_{i\leq s, j\leq r}$ est une base de $E \otimes_k F$ et que Φ est bilinéaire. □

Définition 3.7 (produit tensoriel d'applications linéaires)**.** *Soient E, F, E', F' des k-espaces vectoriels et*

$$\begin{cases} f : E \otimes_k F \longrightarrow E' \\ g : F \otimes_k F \longrightarrow F' \end{cases}$$

des applications linéaires. On considère l'application bilinéaire

$$\begin{array}{rccc} \phi & : & E \times F & \to & E' \otimes_k F' \\ & & (x, y) & \mapsto & f(x) \otimes_k g(y) \end{array}$$

Par la propriété universelle de $E' \otimes_k F'$, il existe une unique application linéaire qu'on note $f \otimes_k g$ telle que

$$\forall (x, y) \in E \times F, (f \otimes_k g)(x \otimes_k y) = f(x) \otimes_k g(y).$$

On appelle $f \otimes_k g$ le produit tensoriel de f et g

Proposition 3.2 (exactitude du produit tensoriel)**.** *Soit*

$$0 \to E' \xrightarrow{i} E \xrightarrow{p} E'' \to 0$$

une suite exacte courte de k-espaces vectoriels, et F un k-espace vectoriel, alors

$$0 \to E' \otimes_k F \xrightarrow{i\otimes_k Id} E \otimes_k F \xrightarrow{p\otimes_k Id} E'' \otimes_k F \to 0$$

est encore exacte.

Démonstration. Soit $(f_1, ..., f_r)$ une base de F, l'injectivité de $i \otimes_k Id$ et la surjectivité de $p \otimes_k Id$ découlent immédiatement de l'existence et l'unicité de l'écriture des éléments de $E \otimes_k F$ donnée dans la propriété-définition.
Soit $x = \sum_{i=1}^{r} x_i \otimes_k f_i \in \ker(p \otimes_k Id)$, alors

$$\begin{aligned} (p \otimes_k Id)(\sum_{i=1}^{r} x_i \otimes_k f_i) &= \sum_{i=1}^{r} p(x_i) \otimes_k f_i \\ &= 0 \end{aligned}$$

par unicité de cette écriture, $\forall i \in [\![1,r]\!]$, $p(x_i)=0$, donc $x_i \in Im(i)$ et donc $\forall i \in [\![1,r]\!]$, il existe $y_i \in E'$ tel que $x_i = i(y_i)$, d'où :

$$\begin{aligned}\sum_{i=1}^{r} x_i \otimes_k f_i &= \sum_{i=1}^{r} i(y_i) \otimes_k f_i \\ &= (i \otimes_k Id)(\sum_{i=1}^{r} y_i \otimes_k f_i)\end{aligned}$$

Donc $\ker(p \otimes_k Id) \subset Im(i \otimes_k Id)$ et le même calcul dans le sens inverse montre l'inclusion réciproque. □

Corollaire 1 Soient E et F des k-espaces vectoriels, et $(M_\alpha)_{\alpha \in A}$ une famille finie de sous-espaces vectoriels de E, alors on a :

$$(\bigcap_{\alpha \in A} M_\alpha) \otimes_k F = \bigcap_{\alpha \in A} (M_\alpha \otimes_k F)$$

Démonstration. L'inclusion directe est immédiate, montrons l'inclusion réciproque :
Soit $x = \sum_{i=1}^{r} x_i \otimes_k f_i$ dans le membre de droite, et soit $\alpha \in A$, on a $\sum_{i=1}^{r} x_i \otimes_k f_i \in M_\alpha \otimes_k F$, donc pour tout $i \in [\![1,r]\!]$, $x_i \in M_\alpha$, et donc $x_i \in \bigcap_{\alpha \in A} M_\alpha$ donc x est dans le membre de gauche. □

Corollaire 2 Soient E et F des k-espaces vectoriels, $(M_\alpha)_{\alpha \in A}$ (resp $(N_\beta)_{\beta \in B}$) une famille finie de sous-espaces vectoriels de E (resp F), alors on a :

$$(\bigcap_{\alpha \in A} M_\alpha) \otimes_k (\bigcap_{\beta \in B} N_\beta) = \bigcap_{(\alpha,\beta) \in A \times B} (M_\alpha \otimes_k N_\beta)$$

Démonstration. On utilise le corollaire 1, en remarquant que si G et H sont des k-espaces vectoriels, alors $G \otimes_k H = H \otimes_k G$. □

Définition 3.8. *Si A et B sont deux k-algèbres, on muni $A \otimes_k B$ d'une structure de k-algèbre en posant $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ et en prolongeant cette définition à $A \otimes_k B$ en respectant la distributivité.*

Proposition 3.3. *Soient A et B deux k-algèbres de dimension finie, alors $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$*

Démonstration. L'inclusion de droite à gauche est évidente, montrons l'inclusion directe :
Soit $x \in Z(A \otimes_k B)$, on écrit $x = \sum_{i=1}^{r} a_i \otimes b_i$. On peut supposer que r est minimal, et dans ce cas, $(b_1, ..., b_r)$ est libre. Soit alors $d \in A$, on a :

$$(d \otimes 1)x - x(d \otimes 1) = \sum_{i=1}^{r} (a_i d - d a_i) \otimes b_i = 0$$

Or $(b_1, ..., b_r)$ est libre donc l'égalité ci-dessus impose que pour tout $i \in [\![1,r]\!]$, $a_i d - d a_i = 0$ et ce pour tout $d \in A$ et donc les a_i sont donc bien dans $Z(A)$. On montre de même que les b_i sont dans $Z(B)$ et on obtient la conclusion. □

Proposition 3.4. *Soit k un corps et n, m deux entiers naturels, on a :*

$$\mathscr{M}_n(k) \otimes_k \mathscr{M}_m(k) \cong \mathscr{M}_{nm}(k)$$

Démonstration. On pose

$$\begin{array}{rccc} \Phi & : & \mathscr{M}_n(k) \times \mathscr{M}_m(k) & \to & \mathscr{M}_{nm}(k) \\ & & (A,B) & \mapsto & \Phi(A,B) \end{array}$$

où, pour $A = (a_{i,j}) \in \mathscr{M}_n(k)$, et $B = (b_{i,j}) \in \mathscr{M}_m(k)$,

$$\Phi(A,B) = \begin{pmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ \vdots & \ddots & \vdots \\ a_{n,1}B & \cdots & a_{n,n}B \end{pmatrix} \in \mathscr{M}_{nm}(k)$$

Remarquons que en notant respectivement $(E_{i,j})$, $(F_{i,j})$ et $(\mathscr{E}_{i,j})$ les bases canoniques de $\mathscr{M}_n(k)$, $\mathscr{M}_m(k)$ et $\mathscr{M}_{nm}(k)$, on a

$$\Phi(E_{i,j}, F_{k,l}) = \mathscr{E}_{ni+k,nj+l}$$

Inversement, si $(i,j) \in [\![1, nm]\!]^2$, on note $i = nq_i + r_i$ et $j = nq_j + r_j$ leurs divisions euclidiennes par n, et on a :

$$\mathscr{E}_{i,j} = \Phi(E_{q_i,q_j}, F_{r_i,r_j})$$

Revenons à la preuve, il suffit de vérifier que $(\mathscr{M}_{nm}(k), \Phi)$ vérifie la propriété universelle du produit tensoriel :
Soient V un k-espace vectoriel, et φ une application bilinéaire de $\mathscr{M}_n(k) \times \mathscr{M}_m(k)$ dans V.
Nécessairement, si f est linéaire de $\mathscr{M}_{nm}(k)$ dans V est telle que $\varphi = f \circ \Phi$, alors d'après la remarque précédente (avec les mêmes notations)

$$\forall (i,j) \in [\![1, nm]\!]^2,\ f(\mathscr{E}_{i,j}) = f(\Phi(E_{q_i,q_j}, F_{r_i,r_j})) = \varphi(E_{q_i,q_j}, F_{r_i,r_j})$$

d'où l'unicité d'une telle application, de plus, toujours d'après la remarque, cette application convient. $(\mathscr{M}_{nm}(k), \Phi)$ est donc bien le produit tensoriel sur k de $\mathscr{M}_n(k)$ et $\mathscr{M}_m(k)$. □

Montrons enfin une proposition technique qui sera cruciale pour notre étude :

Proposition 3.5. *Soit k un corps, A, B deux k-algèbres, et K une extension finie de k, on a*

$$(A \otimes_k B) \otimes_K (B \otimes_k B) \cong (A \otimes_k B) \otimes_k K$$

Démonstration. $(A \otimes_k B) \otimes_K (B \otimes_k B)$ et $(A \otimes_k B) \otimes_k K$ sont munis d'une structure de K-espaces vectoriels, en notant $(a_i)_{1 \leq i \leq n}$ une k-base de A et $(b_j)_{1 \leq j \leq m}$ une k-base de B, on a $((a_i \otimes_k 1) \otimes_K (b_j \otimes_k 1))$ est une K-base de $(A \otimes_k B) \otimes_K (B \otimes_k B)$ et $((a_i \otimes b_j) \otimes_k 1)$ est une K-base de $(A \otimes_k B) \otimes_k K$ (cela se voit sur l'expression d'une base d'un produit tensoriel donnée dans la propriété-définition).
De là, les bases ayant la même taille, ces deux espaces sont isomorphes en tant que K-espaces vectoriels, de surcroît, l'application qui à $(a_i \otimes_k 1) \otimes_K (b_j \otimes_k 1)$ fait correspondre $(a_i \otimes b_j) \otimes_k 1$ est un isomorphisme d'algèbre, d'où la conclusion. □

3.3 Le théorème de Wedderburn

Dans ce paragraphe, on travaille toujours avec un corps k et on se propose de démontrer le résultat suivant :

Théorème 3.1 (d'Artin-Wedderburn)**.** *Soit A une k-algèbre simple de dimension finie, alors il existe un entier $n > 0$ et une algèbre à division D contenant k tels que $A \cong \mathscr{M}_n(D)$, de plus D est unique à isomorphisme près.*

pour prouver ce théorème, on va commencer par prouver 3 lemmes :

Lemme de Schur : Soit M un module simple sur une k-algèbre A, alors $End_A(M)$ est une algèbre à division.

Démonstration. Soit $\varphi \in End_A(M)$ non nulle, on a $\ker\varphi$ et $Im\varphi$ sont des sous-A-modules de M, l'hypothèse $\varphi \neq 0$ implique $\ker\varphi \neq M$ et $Im\varphi \neq \{0\}$ et la simplicité de M impose $\ker\varphi = \{0\}$ (donc φ est injective) et $Im\varphi = M$ (donc φ est surjective), donc φ est inversible. □

De là, si M est un A-module à gauche, on note $D = End_A(M)$, et M est muni d'une structure de D-module en posant :

$$\varphi.x = \varphi(x) \text{ pour tout } \varphi \in D \text{ et tout } x \in M$$

On peut donc considérer l'anneau $End_D(M)$, soit alors $a \in A$, montrons que $(x \mapsto ax) \in End_D(M)$:
Soit $\varphi \in D$ et $x, y \in M$,

$$a(\varphi.x + y) = a\varphi(x) + ay = \varphi(ax) + ay = \varphi.ax + ay$$

De là, on définit un morphisme d'anneaux par :

$$\begin{array}{rccc} \lambda_M & : & A & \to & End_D(M) \\ & & a & \mapsto & (x \mapsto ax) \end{array}$$

Montrons alors le

Lemme de Rieffel : Soit L un idéal à gauche non nul d'une k-algèbre simple A, et soit $D = End_A(L)$, alors λ_L (on peut voir L comme un A-module) est un isomorphisme.

Démonstration. Déjà, $\lambda_L \neq 0$ et A est simple, donc λ_L est injectif.
Montrons que $\lambda_L(L)$ est un idéal à gauche de $End_D(L)$: Soit $\varphi \in End_D(L)$ et $l \in L$, pour tout $x \in M$, $\varphi.\lambda_L(l)(x) = \varphi(lx)$.
Or pour $x_L \in L$, $y \mapsto yx_L$ est dans $D := End_A(L)$ donc par D-linéarité de φ, on a $\varphi(lx) = \varphi(l)x$ et donc $\varphi.\lambda_L(l) = \lambda_L(\varphi(l))$.
$\lambda_L(L)$ est donc bien un idéal à gauche de $End_D(L)$.
De là, on remarque que LA est un idéal bilatère de A car L en est un idéal à gauche et A un idéal à droite, et LA est non nul car L est non nul, donc $LA = A$ par simplicité de A. En particulier, $1 \in LA$ donc il existe $(l_1, ..., l_r)$ des éléments de L et $(a_1, ...a_r)$ des éléments de A tels que $1 = \sum_{i=1}^{r} l_i a_i$.
Soit $\phi \in End_D(L)$,

$$\begin{aligned} \phi &= \phi Id \\ &= \phi\lambda_L(1) \\ &= \phi\lambda_L(\sum_{i=1}^{r} l_i a_i) \\ &= \sum_{i=1}^{r} \underbrace{\phi\lambda_L(l_i)}_{\in\lambda_L(L)} \lambda_L(a_i) \\ &\in \lambda_L(A) \end{aligned}$$

d'où la surjectivité, et la conclusion. □

Enfin, si D est une algèbre à division, soit $n \in \mathbb{N}*$ et I_1 l'ensemble des matrices carrées de taille n ayant des coefficients non nuls uniquement sur la première colonne,
lemme Tout $\mathscr{M}_n(D)$-module à gauche simple est isomorphe à I_1

On peut maintenant passer à la preuve du théorème de Wedderburn :

Démonstration. (Avec les notations de l'énoncé) A est de dimension finie donc une chaîne descendante d'idéaux à gauche non nuls fini par être stationnaire (la suite des dimensions de tels idéaux est à valeurs entières naturelles). Soit donc L un idéal à gauche minimal, non nul, c'est un A-module simple, par le lemme de Schur, $D := End_A(L)$ est une algèbre à division (contenant k), et par le lemme de Rieffel, on a un isomorphisme $A \cong End_D(L)$, de là, si n est la dimension de L en tant que D-module, par le choix d'une base de A, on a $End_D(L) \cong \mathscr{M}_n(D)$.
Reste à montrer l'unicité : Si D et D' sont tels qu'il existe n, m tels que $\mathscr{M}_n(D) \cong A \cong \mathscr{M}_m(D')$, alors l'idéal minimal L explicité ci-dessus est un $\mathscr{M}_n(D)$-module à gauche simple (resp $\mathscr{M}_m(D')$-module à gauche simple) donc

$$\begin{cases} L \cong D^n \\ L \cong D'^m \end{cases}$$

et donc

$$End_A(D^n) \cong End_A(L) \cong End_A(D'^m)$$

Enfin, on pose $\begin{array}{rccc} \varphi & : & D & \to & End_A(D^n) \\ & & d & \longmapsto & ((x_1, ..., x_n) \mapsto (dx_1, ...dx_n)) \end{array}$ φ est bien définie, et est un morphisme d'algèbre injectif.
De plus, soit $f \in End_A(D^n)$, on pose e_i le vecteur de D^n avec tous ses coefficients nuls sauf le i-éme qui vaut 1 et $(E_{i,j})_{1 \leq i,j \leq n}$ la base canonique de $\mathscr{M}_n(D)$, on a :

$$f(e_i) = \sum_{j=1}^{n} a_{i,j} e_j \text{ avec les } a_{i,j} \text{ dans } D$$

Et pour tout $k, j \in [\![1, n]\!]$, par $\mathscr{M}_n(D)$-linéarité de f, on a

$$\begin{aligned} f(E_{j,k}e_1) &= E_{j,k} f(e_1) \\ &= E_{j,k} \sum_{l=1}^{n} a_{1,l} e_l \\ &= \sum_{l=1}^{n} a_{1,l} E_{j,k} e_l \\ &= \sum_{l=1}^{n} a_{1,l} \delta_k^l e_j \\ &= a_{1,k} e_j \end{aligned}$$

D'autre part, $f(E_{j,k}e_1) = f(\delta_k^1 e_j) = \delta_k^1 f(e_j)$
de là, $\forall k, j \in [\![1, n]\!]$, $\delta_k^1 f(e_j) = a_{1,k} e_j$
En prenant $k = 1$, on obtient $f = \varphi(a_{1,1})$, donc φ est surjective et donc $D \cong End_A(D^n) \cong End_A(D'^m) \cong D'$ d'où l'unicité. □

Le cas particulier des corps algébriquement clos :

Théorème 3.2. *Soit k un corps algébriquement clos, alors toute algèbre centrale simple sur k est isomorphe à $\mathscr{M}_n(k)$ pour un certain $n \geq 1$.*

Démonstration. Pour montrer ceci, en utilisant le théorème de Wedderburn, il est suffisant de montrer que la seule k-algèbre à division de dimension finie contenant k est k lui-même.
Soit D une telle k-algèbre, soit $d \in D$, on considère $\varphi_d : \begin{array}{l} k[X] \to D \\ P \mapsto P(d) \end{array}$ le morphisme d'évaluation en d.
Le noyau de φ_d est un idéal de $k[X]$ engendré par un polynôme irréductible P_0 de $k[X]$ (car D est intègre). Et φ_d induit un isomorphisme de k-algèbres entre $k[X]/(P_0)$ et l'image de φ_d, or cette image contient d (le polynôme $X \in k[X]$ convient) et comme k est algébriquement clos, P_0 est de degré 1, et donc $k[X]/(P_0) \cong k$.
On en déduit que $d \in k$, donc $D = k$, ce qui termine la preuve. □

3.4 Corps de décomposition d'une algèbre centrale simple

Passons maintenant à une caractérisation cruciale des algèbres centrales simples :

Théorème 3.3 (de déploiement)**.** *Soit A une k-algèbre de dimension finie, alors A est centrale simple si et seulement si il existe $\mathbb{K}$ une extension finie de k et $n > 0$ tels que $A \otimes_k \mathbb{K} \cong \mathscr{M}_n(\mathbb{K})$*

On va commencer par prouver le
lemme :
Soit A une k-algèbre de dimension finie et $\mathbb{K}$ une extension finie de k, alors A est centrale simple sur k si et seulement si $A \otimes_k \mathbb{K}$ est centrale simple sur $\mathbb{K}$.

Démonstration. Commençons par le sens indirect : si I est un idéal bilatère non trivial de A, alors $I \otimes_k \mathbb{K}$ est un idéal bilatère non trivial de $A \otimes_k \mathbb{K}$. De plus, par la proposition 3.3, $A \otimes_k \mathbb{K}$ est centrale sur $\mathbb{K}$ si et seulement si A est centrale sur k.
Reste donc à prouver que si A est simple, alors $A \otimes_k \mathbb{K}$ l'est. Commençons par remarquer que si A est centrale simple sur k, par le théorème de Wedderburn, il existe $n > 0$ et D une algèbre à division contenant k tels que $A \cong \mathscr{M}_n(D)$ Donc

$$A \otimes_k \mathbb{K} \cong \mathscr{M}_n(D) \otimes_k \mathbb{K} \cong \mathscr{M}_n(k) \otimes_k \mathbb{K} \otimes_k D \cong \mathscr{M}_n(D \otimes_k \mathbb{K})$$

De là, si on suppose que le lemme est vrai pour les algèbres à division, alors $D \otimes_k \mathbb{K}$ est simple, et par l'exemple 2, on a bien $\mathscr{M}_n(D \otimes_k \mathbb{K})$ est simple et il en va de même pour $A \otimes_k \mathbb{K}$.
Montrons le lemme pour D une algèbre à division :
Considérons $(w_1, ..., w_n)$ une k-base de $\mathbb{K}$, alors $(1 \otimes w_1, ..., 1 \otimes w_n)$ est une D-base de $D \otimes_k \mathbb{K}$ en tant que D-espace vectoriel à gauche. Soit alors J un idéal non nul de $D \otimes_k \mathbb{K}$ généré par $z_1, ..., z_r$, on peut que supposer ces éléments sont D-libre et, par le théorème de la base incomplète, les étendre en une D-base de $D \otimes_k \mathbb{K}$ en complétant avec des $1 \otimes w_i$, sans restreindre la généralité, supposons que $(z_1, ..., z_r, 1 \otimes w_{r+1}, ..., 1 \otimes w_n)$ est une base de $D \otimes_k \mathbb{K}$.
Alors, pour $i \in [\![1, r]\!]$, il existe $\alpha_{i,r+1}, ..., \alpha_{i,n}$ dans D tels que

$$1 \otimes w_i = \sum_{j=r+1}^{n} \alpha_{i,j}(1 \otimes w_j) + y_i$$

où y_i est une combinaison linéaire des z_k donc un élément de J. De plus, $y_1, ..., y_r$ sont D-linéairement indépendants car les $1 \otimes w_1, ..., 1 \otimes w_n$ le sont. Donc $(y_1, ..., y_r)$ est une D-base de J.
Soit $d \in D$, comme J est un idéal bilatère, pour tout $1 \leq i \leq r$ $d^{-1}y_i d$ est dans J, donc il existe $(\beta_{i,l})_{1 \leq l \leq r}$ tels que

$$d^{-1}y_i d = \sum_{l=1}^{r} \beta_{i,l} y_l$$

En utilisant les expressions des y_i, on obtient :

$$1 \otimes w_i - \sum_{j=r+1}^{n} d^{-1}\alpha_{i,j} d(1 \otimes w_j) = \sum_{l=1}^{r} \beta_{i,l}(1 \otimes w_l) - \sum_{l=1}^{r} \beta_{i,l} \sum_{j=r+1}^{n} \alpha_{l,j}(1 \otimes w_j)$$

Et en utilisant l'indépendance des $1 \otimes_k w_j$, on obtient $\beta_{i,i} = 1$ et $\beta_{i,l} = 0$ si $l \neq i$, et $d^{-1}\alpha_{i,j}d = \alpha_{i,j}$ et ce pour tout $d \in D$, et comme D est centrale sur k, $\alpha_{i,j} \in k$.
Enfin, on en déduit que $\forall i \in [\![1, r]\!]$,

$$\begin{aligned} y_i &= 1 \otimes w_i - \sum_{j=r+1}^{n} \alpha_{i,j}(1 \otimes w_j) \\ &= 1 \otimes w_i - \sum_{j=r+1}^{n} (1 \otimes \alpha_{i,j} w_j) \\ &= 1 \otimes (w_i - \sum_{j=r+1}^{n} \alpha_{i,j} w_j) \\ &\in \mathbb{K} \end{aligned}$$

$\mathbb{K}$ étant un corps, on a $J \cap \mathbb{K} = \mathbb{K}$ donc $1 \otimes 1 \in J$ donc $J = D \otimes_k \mathbb{K}$ d'où la conclusion. □

Preuve du théorème de déploiement. Le sens indirect découle immédiatement du lemme précédent et de l'exemple 2 traité au début de la partie. Montrons le sens direct :
On note $\overline{k}$ une clôture algébrique de k, montrons que $A \otimes_k \overline{k}$ est central simple sur $\overline{k}$, déjà son centre est $\overline{k}$ car A est centrale sur k. Soit J un idéal non trivial de $A \otimes_k \overline{k}$, soit alors $\lambda \in \overline{k}$, montrons que $1 \otimes \lambda \in J$: On pose $K = k(\lambda)$, cette extension est de dimension finie sur k car tous les éléments de $\overline{k}$ sont algébriques sur k, donc par le lemme $A \otimes K$ est centrale simple sur K. De là, $J \cap (A \otimes K)$ est un idéal bilatère de $A \otimes K$ et si celui-ci est nul, alors pour toute extension finie K' de k contenant K, $J \cap (A \otimes K')$ sera aussi nul (car c'est un idéal de $A \otimes K'$ qui est simple par le lemme) donc $J \cap (A \otimes K)$ est un idéal bilatère non nul de $A \otimes K$ qui est simple, donc $J \cap (A \otimes K) = (A \otimes K)$ ce qui donne que J contient tous les $A \otimes K$ pour K une extension finie de k, et donc $J = A \otimes_k \overline{k}$ donc $A \otimes_k \overline{k}$ est simple.

Par le corollaire du théorème de Wedderburn pour les corps algébriquement clos, on a : $A \otimes_k \overline{k} \cong \mathscr{M}_n(\overline{k})$ pour un certain $n > 0$. De là, comme $A \otimes_k \overline{k}$ est l'union des $A \otimes_k K$ où K est une extension finie

de k contenue dans $\overline{k}$, pour une extension finie K_0 de degré suffisamment grand, $A \otimes_k K_0$ contient les éléments $e_1, ..., e_{n^2}$ de la base canonique de $\mathscr{M}_n(\overline{k})$. En associant ces éléments à la base canonique de $\mathscr{M}_n(K_0)$ on obtient un isomorphisme de $A \otimes_k K_0$ vers $\mathscr{M}_n(K_0)$. □

Corollaire immédiat : Si A est centrale simple sur k alors sa dimension sur k est un carré.

Théorème 3.4 (Noether, Köthe)**.** *[PG04][P.22] Une k-algèbre centrale simple a un corps de déploiement séparable sur k.*

Corollaire :[PG04][P.22] Une k-algèbre de dimension finie A est centrale simple si et seulement si il existe $n \in \mathbb{N}^*$ et une extension galoisienne finie $K|k$ tels que $A \otimes_k K \cong \mathscr{M}_n(K)$.

Définition 3.9. *Soit A une algèbre centrale simple sur k, une extension finie $K|k$ telle que $A \otimes K \cong \mathscr{M}_n(K)$ pour un certain $n > 0$ est appelé corps de rupture de A, et l'entier $\sqrt{dim_k A}$ est appelé le degré de A sur k.*

Proposition 3.6. *Soit K une extension de k et A, B deux algèbres centrales simples dont K est un corps de déploiement, alors K est un corps de déploiement de $A \otimes_k B$.*

Démonstration. On note n (resp m) l'entier tel que $A \otimes_k K \cong \mathscr{M}_n(K)$ (resp $B \otimes_k K \cong \mathscr{M}_m(K)$, alors au vu des propositions **3.4** et **3.5**, on a :

$$\begin{aligned}(A \otimes_k B) \otimes_k K &\cong (A \otimes_k B) \otimes_K (B \otimes_k B) \\ &\cong \mathscr{M}_n(K) \otimes_K \mathscr{M}_m(K) \\ &\cong \mathscr{M}_{nm}(K)\end{aligned}$$

□

Enfin, on va noter $CSA_K(n)$ l'ensemble des k-algèbres centrales simples de degré n déployées par K, on peut reformuler la propriété précédente :

Soient m, n des entiers naturels non nuls, le produit tensoriel est une application de
$CSA_K(n) \times CSA_K(m)$ dans $CSA_K(nm)$

de là, on définit une relation d'équivalence sur $\bigcup_{n\in\mathbb{N}^*} CSA_K(n)$:

Définition 3.10. *Soient A et (resp B) dans $\bigcup_{n\in\mathbb{N}^*} CSA_K(n)$, et soient D et (resp D') l'unique k-algèbre à division telle que $A \cong \mathscr{M}_n(D)$ (resp $B \cong \mathscr{M}_m(D')$), A et B sont dites Brauer-équivalentes si $D \cong D'$.*

Proposition 3.7. *La "Brauer-équivalence" est une relation d'équivalence, et pour A et B deux k-algèbres centrales simples, A et B sont Brauer-équivalentes si et seulement si il existe $n, m \in \mathbb{N}^*$ tels que $A \otimes_k \mathscr{M}_n(k) \cong B \otimes_k \mathscr{M}_m(k)$.*

Démonstration. Le fait que cette relation est une relation d'équivalence provient essentiellement de l'unicité du théorème de Wedderburn, passons à la caractérisation :
Pour l'implication directe, posons $A \cong \mathscr{M}_n(D)$ et $B \cong \mathscr{M}_m(D')$, on a alors :

$$\begin{aligned}A \otimes_k \mathscr{M}_m(k) &\cong \mathscr{M}_n(D) \otimes_k \mathscr{M}_m(k) \\ &\cong \mathscr{M}_n(k) \otimes_k D \otimes_k \mathscr{M}_m(k) \\ &\cong \mathscr{M}_m(k) \otimes_k D \otimes_k \mathscr{M}_n(k) \\ &\cong \mathscr{M}_m(D) \otimes_k \mathscr{M}_n(k) \\ &\cong B \otimes_k \mathscr{M}_n(k)\end{aligned}$$

Réciproquement, si $A \otimes_k \mathscr{M}_n(k) \cong B \otimes_k \mathscr{M}_m(k)$, en notant D (resp D') l'algèbre à division telle que $A \cong \mathscr{M}_r(D)$ (resp $A \cong \mathscr{M}_s(D')$) alors

$$A \otimes_k \mathscr{M}_n(k) \cong \mathscr{M}_{nr}(D)$$

D'une part, et

$$A \otimes_k \mathscr{M}_n(k) \cong B \otimes_k \mathscr{M}_m(k) \cong \mathscr{M}_{ms}(D')$$

D'autre part, et l'unicité du théorème de Wedderburn donne $D \cong D'$. □

Remarque : On voit aisément (toujours grâce à l'unicité du théorème de Wedderburn) que chaque classe d'équivalence pour cette relation contient une unique k-algèbre à division.

Notons alors $A(K/k)$ l'ensemble $\bigcup_{n\in\mathbb{N}^*} CSA_K(n)$ quotienté par la relation de Brauer-équivalence, et $A(k)$ l'union des $A(K/k)$ pour K parcourant les extensions galoisiennes de k.

Par la remarque précédente, on constate que l'étude de $A(k)$ est équivalente à l'étude des k-algèbres à division. Intéressons nous de plus près à la structure de $A(k)$:

Proposition 3.8. *L'ensemble $A(k)$ muni de la loi de composition induite par le produit tensoriel est un groupe abélien.*

Démonstration. L'associativité et la commutativité de la loi sont héritées de l'associativité et la commutativité du produit tensoriel, l'élément neutre pour cette loi est la classe commune des $\mathscr{M}_n(k)$ pour $n \in \mathbb{N}^*$, reste donc à trouver, étant donnée A une k-algèbre centrale simple, un inverse pour A :

Lemme : Soit A une k-algèbre de dimension $n \in \mathbb{N}^*$, alors A^{OP} est centrale simple, et on a :

$$A \otimes_k A^{OP} \cong End_k(A) \cong \mathscr{M}_n(k)$$

Démonstration. D'une part, le centre de A^{OP} est aussi le centre de A, de plus un sous-A-module à gauche de A est un sous-A^{OP}-module à droite de A^{OP}, donc A est simple si et seulement si A^{OP} l'est. De là, A^{OP} est aussi centrale simple et est déployée par le même corps que A ($A \otimes_k K \cong A^{OP} \otimes_k K$ en temps qu'espace vectoriel, et le produit est renversé) donc $A \otimes_k A^{OP}$ est centrale simple sur k.
En outre, posons

$$\begin{array}{rccc} Sand & : & A \otimes_k A^{OP} & \longrightarrow & End_k(A) \\ & & a \otimes_k b & \longmapsto & (z \mapsto azb) \end{array}$$

qu'on appellera le morphisme *Sandwich*, il est bien défini car $A \otimes_k A^{OP}$ est engendré par ses tenseurs purs, c'est une application k-linéaire, et c'est un morphisme d'algèbre (en effet le produit de A^{OP} est le produit de A renversé).
Par le lemme de Schur, le noyau de $Sand$ est trivial, ce morphisme est donc injectif et comme

$$dim_k(A \otimes_k A^{OP}) = n^2 = dim_k(End_k(A))$$

c'est un isomorphisme. □

On a donc montré que A^{OP} est un inverse de A donc $A(k)$ est bien muni d'une structure de groupe. □

Reste donc a comparer les deux groupes qu'on a construit en partant de k : $A(k)$ et $Br(k)$, c'est l'objectif de la partie suivante.

4 Identification des deux constructions du groupe de Brauer

L'objectif va donc être de montrer que, pour un corps k, on a isomorphisme entre $Br(k)$ et $A(k)$. Expliquons rapidement le schéma de preuve. On montre en premier lieu que les deux groupes en question s'écrivent en fait comme limite inductive de deux systèmes. Ensuite nous verrons par un argument de descente que les éléments des systèmes sont eux isomorphes deux à deux, et en établissant cette correspondance puis en passant à la limite on aura montré que $Br(k)$ et $A(k)$ sont les mêmes objets.

4.1 Limite inductive et projectives

4.1.1 généralités

À la lumière du schéma de preuve, il convient de rappeler quelques propriétés sur les limites inductives et projectives. Comme il ne s'agit pas de ce que nous souhaitons fondamentalement parler, nous n'en donnerons pas les preuves. Toute fois nous préciserons les références utilisées.

Définition 4.1. *Considérons $(I, \leq)$ est un ensemble ordonné filtrant et $(E_i)_{i\in I}$ une famille d'ensembles indexée par I. On suppose aussi que pour $i \leq j$ dans I il existe une application $f_i^j : E_j \to E_i$, de sorte que :*

- *pour tout $i \in I$, $f_i^i = \mathrm{Id}_{E_i}$*
- *pour $i \leq j \leq k$ dans I, $f_i^k = f_i^j \circ f_j^k$.*

On dit alors que le couple $\left((E_i)_{i\in I}, (f_i^j)_{i\leq j}\right)$ est un système projectif. De plus, on appelle limite projective du système et on note $\varprojlim E_i$ l'ensemble :

$$\left\{ x \in \prod_{i\in I} E_i \;\middle|\; \forall i \leq j, f_i^j(x_j) = x_i \right\}.$$

Pour un système projectif, le diagramme suivant, avec $i \leq j \leq k$, est donc commutatif.

$$\begin{array}{ccccccc} \cdots & \longleftarrow & E_i & \xleftarrow{f_i^k} & E_k & \longleftarrow & \cdots \\ & & & \nwarrow^{f_i^j} \quad \swarrow^{f_j^k} & & & \\ & & & E_j & & & \end{array}$$

On définit de la manière duale la notion de *limite injective* notée $\varinjlim E_i$. Visuellement en inversant le "sens" des flèches projectives, on obtient un système injectif dans la catégorie opposée. Ainsi on vérifie que les prochaines propriétés sur les limites projectives se transportent sur les limites injectives.

Un certain nombre de structures algébriques passent à la limite projective, les R-module en particulier. Si $\left((E_i)_{i\in I}, (f_i^j)_{i\leq j}\right)$ est un système projectif tel que tous les E_i sont munis de cette structure et tel que pour tout $i \leq j \in I$, f_i^j est un morphisme, alors $\varprojlim E_i$ est naturellement muni de la même structure. La limite projective possède de bonnes propriétés, au sens où un *"isomorphisme"* entre deux systèmes projectifs se transporte en un isomorphisme entre les limites.

Proposition 4.1. *Soient $\left((E_i)_{i\in I}, (f_i^j)_{i\leq j}\right)$ et $\left((F_i)_{i\in I}, (g_i^j)_{i\leq j}\right)$ deux systèmes projectifs de R-module, indexés par le même I. On suppose que pour tout $i \in I$ il existe un isomorphisme $\phi_i : E_i \to F_i$ qui vérifie pour tout $i \leq j \in I$: $\phi_i \circ f_i^j = g_i^j \circ \phi_j$ (voir diagramme commutatif ci-dessous). Alors $\varprojlim E_i \simeq \varprojlim F_i$.*

$$\begin{array}{ccc} E_i & \xleftarrow{f_i^j} & E_j \\ {\scriptstyle\phi_i}\downarrow & & \downarrow{\scriptstyle\phi_j} \\ F_i & \xleftarrow[g_i^j]{} & F_j \end{array}$$

Proposition 4.2. *Soit (E_i, f_i^j) un système inductif d'une catégorie concrète, on obtient la limite inductive des E_i comme le quotient de l'union disjointe $\bigsqcup_{i\in I} E_i$ par la relation d'équivalence :*

$$(i,x) \sim (j,y) \Leftrightarrow \exists k \in I \text{ tel que } i \leq k, j \leq k \text{ et } f_i^k(x) = f_j^k(y)$$

4.1.2 Pour $Br(k)$ homologique

Si K est une extension galoisienne de groupe de Galois G. Pour toute extension intermédiaire finie galoisienne $k \to F \to K$ on a des groupes de Galois $G_{F/k}$ et $G_{K/F}$. Si on note $H = G_{K/F}$, la théorie de Galois nous dit que l'on a l'égalité :

$$Card(G/H) = Card(G_{F/k}) = [F : k] < \infty$$

et un morphisme canonique

$$G \to G/H$$

Alors par la propriété universelle de la limite projective on a un morphisme :

$$G \to \varprojlim_{H\in\mathscr{H}} G/H$$

Où $\mathscr{H}$ est l'ensemble des groupes de Galois obtenus comme précédemment.

Théorème 4.1. *Le morphisme ainsi construit $G \to \varprojlim G/H$ est un isomorphisme.*

Démonstration. Pour la démonstration nous renvoyons à [Lan] page 313 □

Définition 4.2. *On appelle un tel groupe, obtenu comme limite projective, un groupe* profini.

Symétriquement on montre que la clôture séparable d'un corps est, elle, limite inductive d'extensions naturelles.

Proposition 4.3. *Soit k un corps. On considère la famille des extensions galoisiennes intermédiaires finies K/k, et k^s la clôture séparable de k, alors :*

$$k^s = \varinjlim K/k$$

Ainsi en ayant ces visions *asymptotiques* d'un groupe de Galois infini et d'une clôture séparable, on souhaiterait faire passer les limites inductives et projectives "à travers" le H^2 dans l'expression suivante :

$$Br(k) = H^2(G(k^s/k), k^{s*}) = H^2\left(\varprojlim G(K^s/k)/G(K^s/F), \varinjlim F/k\right)$$

Cette interversion est justifiée par la propriété suivante démontré dans [Har] page 82.

Proposition 4.4. *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 $G = \varprojlim_i G_i$ et $A = \varinjlim_i$. Alors pour tout $q \in \mathbb{N}$*

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

On dit que A est un G-module discret quand l'action de G sur A est continue en munissant A d'une topologie discrète. Ce qui nous va parfaitement car en effet lorsque l'on considère l'action du groupe de Galois absolu d'un corps k sur k^{s*}, on muni ce dernier d'une telle structure discrète.

Et donc on obtient la décomposition cherchée pour le groupe de Brauer cohomologique :

Théorème 4.2.

$$Br(k) = \varinjlim H^2\left(G(K/k), K\right)$$

4.1.3 Pour $A(k)$ par les extensions

On note A_k le groupe de Brauer par les extensions. Si K/k est une extension de k alors par extension des scalaires on obtient $A_k \to A_K$ un homomorphisme. En notant $A(K/k)$ le noyau de ce dernier, on montre que :

$$A_k = \lim_{\to} A(K/k)$$

pour K extensions galoisiennes finies de k. Cette limite inductive est même réunion.

4.2 Démonstration de l'isomorphie

On a vu ces deux constructions comme des limites inductives sur les mêmes systèmes, il faut donc trouver des isomorphismes $A(K/k) \to H^2(K/k)$ faisant commuter le diagramme suivant :

$$(D) := \qquad \begin{array}{ccc} A(K/k) & \longrightarrow & H^2(K/k) \\ \downarrow & & \downarrow \\ A(K'/k) & \longrightarrow & H^2(K'/k) \end{array}$$

C'est à dire compatible avec les injections verticales pour chaque K'/K extensions galoisiennes finies. Nous allons pour ce faire, passer par un groupe intermédiaire noté $H^1(G, PGL_\infty)$ qui sera d'une part isomorphe à $A(K/k)$ et d'autre part isomorphe à $H^2(K/k)$.

4.2.1 Du côté de $A(K/k)$

Une première étape est d'appliquer un principe de descente galoisienne, explicité en annexe. Pour se faire on va "découper" l'ensemble $A(K/k)$ par dimensions. De manière plus rigoureuse :

Définition 4.3. *Pour $n \in \mathbb{N}$, on note $A(n, K/k)$ l'ensemble des classes de k-algèbres A telles que $A \bigotimes_k K \cong M_n(K)$.*

On a donc directement

$$A(K/k) = \bigcup_{n=0}^{+\infty} A(n, K/k)$$

On veut donc a présent interpréter ces $A(n, K/k)$ comme des H^1. La belle idée est donc de voir un élément de $A(n, K/k)$ comme un couple (V, x) avec V un espace de dimension n^2 (qui représente $M_n(K)$) et $x \in V \otimes V^* \otimes V^*$. Pourquoi ? Il s'agit essentiellement de remarquer que x représente la loi de composition de V, en effet comme on a l'isomorphisme :

$$F \otimes E^* \cong \mathscr{L}(E, F) \qquad \text{pour E et F des espaces vectoriels sur un même corps}$$

On obtient :

$$V \otimes V^* \otimes V^* \cong \mathscr{L}(V, V) \otimes V^* \cong \mathscr{L}(V, \mathscr{L}(V, V)) \cong \mathscr{B}(V \times V, V)$$

Ceci dit, si on note $G = Gal(K/k)$ et $C_K = Aut_K(M_n(K))$ par l'argument de descente (5.1) en annexe, on a la bijection

$$\theta : \ A(n, K/k) \longrightarrow H^1(G, C_K)$$

Or tous les K-automorphismes de $M_n(K)$ sont intérieurs donc $C_K \cong GL_n(K)/K^*$, et donc $C_K \cong PGL_n(K)$. D'où la bijection

$$\theta_n : \ A(n, K/k) \longrightarrow H^1(G, PGL_n(K))$$

Soient n, $m \in \mathbb{N}^*$, on a une injection naturelle $GL_n(K) \to GL_{nm}(K)$ envoyant une matrice M de taille n sur $Diag(M, ..., M)$ de taille mn. En passant au quotient par les matrices scalaire, on obtient ainsi des applications :

$$\lambda_{nm} : H^1(G, PGL_n(K)) \to H^1(G, PGL_{nm}(K))$$

Proposition 4.5. *Soient n, m dans $\mathbb{N}^*$ et K/k une extension galoisienne finie, alors le diagramme suivant commute :*

$$\begin{array}{ccc} A(n, K/k) & \xrightarrow[\theta_n]{} & H^1(G, PGL_n(K)) \\ \otimes_k \mathscr{M}_n(k) \downarrow & & \downarrow \lambda_{nm} \\ A(nm, K/k) & \xrightarrow{\theta_{nm}} & H^1(G, PGL_{nm}(K)) \end{array}$$

Démonstration. On le voit en vérifiant que l'opération $M \mapsto Diag(M, \ldots, M)$ est en fait $M \mapsto M \otimes I_m$ □

On remarque alors que les λ_n sont en fait injectives. En effet par le diagramme commutatif précédent, λ_{nm} envoi la classe (dans le H^1) d'une k-algèbre centrale simple A, sur la classe de $A \otimes M_n(k)$. D'où :

Proposition 4.6. *Pour tout $n, m > 0$, l'application λ_{nm} est injective.*

Démonstration. Si A et A' sont deux k-algèbres centrales simples, le théorème de Wedderburn nous assure d'une part que $A = M_n(D)$ et $A' = M_n(D')$. D'autre part si on suppose que $A \otimes M_n(k) \cong A' \otimes M_n(k)$, alors ces dernières sont également des algèbres à divisions sur D et D'. Or par l'unicité dans le théorème de Wedderburn, $D \cong D'$. Et donc $A \cong A'$. □

Il est facile de vérifier en outre, par définition des λ_{ij}, que pour $n, m, l \in \mathbb{N}^*$, $\lambda_{(nm)l} \circ \lambda_{nm} = \lambda_{n(ml)}$

On considère alors le système $(H^1(G, PGL_n(K)))_{n \in \mathbb{N}^*}$ où $\mathbb{N}^*$ est ordonné par la division et pour $d, n \in \mathbb{N}^*$ tels que d divise n,on a $\lambda_{dn/d}$ de $H^1(G, PGL_d(K))$ dans $H^1(G, PGL_n(K))$. On note alors $H^1(G, PGL_\infty)$ la limite inductive des $H^1(G, PGL_d(K))$ selon les λ_{mn}.

Théorème 4.3. *Soit K/k une extension galoisienne finie, alors $H^1(G, PGL_\infty(K))$ est muni d'une structure de groupe et est isomorphe à $A(K/k)$*

Démonstration. Soient $\overline{x}, \overline{y}$ dans $H^1(G, PGL_\infty(K))$, proposition 4.2 sur les limites inductives permet de considérer des relèvements (n, x) (resp.(m, y)) dans $H^1(G, PGL_n(K))$ (resp. $H^1(G, PGL_m(K))$), de là, on a : $\theta_n^{-1}(x) \otimes_k \theta_m^{-1}(y) \in A(nm, K/k)$ et on peut envoyer cette algèbre dans $H^1(G, PGL_{nm}(K))$ via la bijection θ_{nm}, puis renvoyer cette image dans la limite inductive $H^1(G, PGL_\infty(K))$, on note $\overline{x} \times_\infty \overline{y}$ cet élément.
La loi $\times_\infty$ est une loi de composition interne sur $H^1(G, PGL_\infty(K))$ de plus, cette loi est associative et commutative (ces propriétés sont directement héritées des propriétés de la loi de groupe sur $A(K/k)$, soit $n \in \mathbb{N}^*$ l'image dans $H^1(G, PGL_\infty(K))$ de $\theta_n(\mathscr{M}_n(k))$ est un neutre pour cette loi (cette définition ne dépend pas du n choisit car les θ_n sont des bijections pointées et que les diagrammes de la proposition 4.5 commutent). Enfin l'existence d'un inverse pour chaque élément de $H^1(G, PGL_\infty(K))$ provient aussi de l'existence d'un inverse dans $A(K/k)$ et le fait qu'on envoie les préimages du neutre de $A(K/k)$ sur les préimages du neutre de $H^1(G, PGL_\infty(K))$ via les θ_i.
Soit $\overline{x}$ un élément de A(K/k), et x un de ses relèvements dans un $\mathscr{M}_n(k)$ à $\overline{x}$ on associe l'image dans $H^1(G, PGL_\infty(K))$ de $\theta_n(x)$ (gardons à l'esprit que cette image ne dépend pas du n choisit) ceci décrit un isomorphisme de $A(K/k)$ dans $H^1(G, PGL_\infty(K))$.

□

4.2.2 Du côté de $H^2(K/k)$

Ici on a besoin de la cohomologie non abélienne pour passer du $H^1(G, PGL_\infty(K))$ au $H^2(K/k)$, car $GL_n(K)$ n'est pas abélien en général. On identifie dans toute cette partie K^* et l'ensemble des matrices scalaires non nulles. En appliquant la proposition (5.4) de l'annexe à la suite exacte :

$$1 \longrightarrow K^* \xrightarrow{i} GL_n(K) \xrightarrow{\pi} PGL_n(K) = C_K \longrightarrow 1$$

on obtient un opérateur de cobord :

$$\Delta_n \ : \ H^1(G, PGL_n(K)) \to H^2(G, K^*)$$

Proposition 4.7. *Les application Δ_n sont compatibles entre elles, et définissent un* morphisme *:*

$$\Delta : \ H^1(G, PGL_\infty(K)) \to H^2(K/k)$$

Démonstration. En premier lieu, il s'agit de voir en quel sens les Δ_n sont-elles compatibles entre elles :

On vérifie que le diagramme suivant est commutatif

$$\begin{array}{ccc} H^1(G, PGL_n(K)) & \xrightarrow{\Delta_n} & H^2(G, K^*) \\ \downarrow \quad \lambda_{nm} & & \downarrow id \\ H^1(G, PGL_{nm}(K)) & \xrightarrow{\Delta_{nm}} & H^2(G, K^*) \end{array}$$

En effet la classe d'un cocycle c dans $H^1(G, PGL_n(K))$ est envoyé par construction de Δ_n sur la classe d'un 2-cocycle a : $(s,t) \mapsto a_{s,t} = b_s s(b_t) b_{st}^{-1}$ avec pour $s, t \in G$, $b_s \in GL_n(K)$ et $a_{s,t} \in K^*$. En identifiant $a_{s,t}$ avec sa matrice scalaire, alors en encore une fois en appliquant λ_{nm} on regarde la classe de $Diag(a_{s,t}I_n, ..., a_{s,t}I_n) = a_{s,t}I_{nm}$, donc ce sont les mêmes vus dans K^*.

Comme on a déjà montré que les λ_n sont injectives, en prenant la limite inductive sur les $H^1(G, PGL_n(K))$ on peut effectivement définir Δ comme application.

Il s'agit maintenant de voir en quoi Δ respecte les structures de groupes de $H^1(G, PGL_\infty(K))$ et $H^2(K/k)$.On note l'opération de produit :

$$\times : \ H^1(G, PGL_n(K)) \times H^1(G, PGL_m(K)) \to H^1(G, PGL_{nm}(K))$$

induite par le produit tensoriel sur les $A(n, K/k)$ et la structure de groupe de $H^1(G, PGL_\infty)$, compatible aux λ_n.Nous allons montrer que pour $\tilde{c} \in H^1(G, PGL_n(K))$ et $\tilde{d} \in H^1(G, PGL_m(K))$ on a :

$$\Delta_{nm}(\tilde{c} \times \tilde{d}) = \Delta_n(\tilde{c})\, \Delta_m(\tilde{d})$$

Par construction on sait que $c' : (s,t) \mapsto b_s.s(b_t).b_{st}^{-1}$ est un représentant de la classe de $\Delta_n(\tilde{c})$, avec b un antécédent de c (où c représente $\tilde{c}$) au sens :

$$\forall s \in G \, \pi(b_s) = c_s$$

Avec donc $b_s \in GL_n(K)$.On peut alors voir $\Delta_n(\tilde{c})$ comme suit :

$$\begin{aligned} \Delta_n(\tilde{c}) &= Classe[(s,t) \mapsto b_s.s(b_t).b_{st}^{-1}] \\ &= Classe[(s,t) \mapsto \mu_{s,t}] \qquad \mu_{s,t} \in K^* \end{aligned}$$

et de même :

$$\Delta_m(\tilde{d}) = Classe[(s,t) \mapsto \nu_{s,t}]$$

Intéressons nous maintenant à ce qu'il se passe dans le premier membre de l'équation. Comme $\times$ est induite par le produit tensoriel on a

$$\Delta_{nm}(\tilde{c} \times \tilde{d}) = Classe[(s,t) \mapsto m_{\mu_{s,t}} \otimes m_{\nu_{s,t}}]$$

Où m_x : est l'application linéaire donnée par la multiplication par x. Or ce tenseur $m_{\mu_{s,t}} \otimes m_{\nu_{s,t}}$ est représentée par la matrice scalaire $\mu_{s,t}\nu_{s,t}I_{nm}$, et donc par le $2-cocycle : (s,t) \mapsto \mu_{s,t}\nu_{s,t}$. On a donc bien

$$\Delta_{nm}(\tilde{c} \times \tilde{d}) = Classe[(s,t) \mapsto \mu_{s,t}\nu_{s,t}] = Classe[(s,t) \mapsto \mu_{s,t}].Classe[(s,t) \mapsto \nu_{s,t}] = \Delta_n(\tilde{c}).\Delta_m(\tilde{d})$$

Ainsi par passage à la limite, on obtient que Δ est un morphisme.

□

Théorème 4.4. *Le morphisme Δ est bijectif.*

Démonstration. Vérifions l'injectivité, en se ramenant au cas des Δ_n. Par construction de Δ_n on a la suite exacte :

$$H^1(G, GL_n(K)) \xrightarrow{\pi_1} H^1(G, PGL_n(K)) \xrightarrow{\Delta_n} H^2(G, A)$$

Or le théorème 90 de Hilbert (2.8) nous assure que $H^1(G, GL_n(K))$ est nul, et donc que Δ_n est injectif. On conclut par passage à la limite.

De même montrons que si on fixe $n = [K : k] = Card(G)$, alors Δ_n est surjective. Soit $a : G \times G \to K^*$ un 2-cocycle Il s'agit donc de montrer que a s'écrit :

$$a_{s,t} = b_s s(b_t) b_{st}^{-1} \qquad \text{où pour tout } \ s \in G,\ b_s \in GL_n(K)$$

On considère alors V un espace vectoriel sur K dont une base $(e_s)_{s\in G}$ est indexée par G. On considère alors l'endomorphisme de V :

$$b_s :\ e_t \mapsto a_{s,t}e_{st}$$

On remarque alors que pour $s, t, u \in G$:

$$\begin{aligned} b_s s(b_t)(e_u) =& b_s\left(s(a_{t,u}).e_{tu}\right) \\ =& s(a_{t,u})\, b_s(e_{tu}) \\ =& s(a_{t,u}) a_{s,tu} e_{stu} \end{aligned}$$

Et également :

$$a_{s,t}b_{st}(e_u) = a_{s,t}a_{st,u}e_{stu}$$

Or a est un 2-cocycle donc :

$$s(a_{t,u}) = a_{st,u}a_{s,tu}^{-1}a_{s,t}$$

Ainsi on trouve :

$$\begin{aligned} b_s s(b_t)(e_u) =& a_{st,u}a_{s,tu}^{-1}a_{s,t}a_{s,tu}e_{stu} \\ =& a_{st,u}a_{s,t}e_{stu} \\ =& a_{s,t}b_{st}(e_u) \end{aligned}$$

Et donc comme souhaité

$$b_s s(b_t) b_{st}^{-1} = a_{s,t}$$

d'où la surjectivité de Δ_n et donc de Δ. On peut donc conclure que Δ est un isomorphisme !

□

4.2.3 Conclusion

Finalement, on a montré que les groupes $H^1(G, PGL_\infty(K))$ et $A(K/k)$ sont isomorphes et ce pour toute extension galoisienne finie K/k d'autre part, Δ est un isomorphisme de $H^1(G, PGL_\infty(K))$ dans $H^2(G, K)$. On a donc un isomorphisme entre $A(K/k)$ et $H^2(G, K)$, on peut en outre passer à la limite inductive sur les extensions galoisiennes finies de k et conserver l'isomorphisme grâce à la commutativité du diagramme (D) du début de la section 4.2, et par le théorème 4.2, on a :

$$A(k) \cong \varinjlim A(K/k) \cong \varinjlim H^2(G, K) \cong Br(k)$$

D'où l'équivalence des deux constructions.

4.2.4 Quelques calculs de groupe de Brauer

Soit k un corps algébriquement clos, le théorème de Wedderburn de la section 3 et son corollaire montre qu'il n'existe pas d'algèbre centrale simple sur K autre que les $\mathscr{M}_n(K)$ pour $n \in \mathbb{N}^*$ donc le groupe de Brauer d'un tel corps est trivial.

Soit k un corps fini, un autre théorème de Wedderburn permet d'affirmer qu'il n'existe pas d'algèbre à division centrale sur k de dimension finie sur k (plus précisément une algèbre à division finie est toujours un corps) ce qui permet de conclure encore une fois que le groupe de Brauer de k est trivial.

Dans le cas où $k = \mathbb{R}$, un théorème de Frobenius (1877) dit qu'il n'existe que 3 algèbres associative à division sur $\mathbb{R}$: $\mathbb{R}$ lui-même, $\mathbb{C}$ et l'algèbre des quaternions $\mathbb{H}$, de plus $\mathbb{R}$ et $\mathbb{H}$ sont les seules à être centrales sur $\mathbb{R}$. Le groupe de Brauer de $\mathbb{R}$ est donc d'ordre 2, d'où

$$Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$$

5 Annexe

5.1 Cohomologie galoisienne non abélienne

On considère toujours G et $(A, .)$ des groupes, avec G agissant sur A, action notée $g(a)$ pour rappeler celle du groupe de Galois. Mais à la différence de la théorie des G-modules, on ne suppose pas que A est abélien. Nous allons voir que nous pouvons quand même dire des choses jusqu'au deuxième ensemble (et pas groupe !) de cohomologie. On essaye de prolonger ce que l'on sait sur le calcul homologique au moyen de cochaîne (voir l'annexe).

Définition 5.1. *On définit tout d'abord, par analogie avec le cas abélien :*

$$H^0(G, A) = A^G = \{a \in A \mid \forall s \in G \; s(a) = a\}$$

les invariants pour l'action de G.

Définition 5.2. *On appelle* cocycle *une application $a : G \to A$ telle que pour $s, t \in G$ $a_{st} = a_s.s(a_t)$ (on note l'évaluation d'un cocycle en indice, pour ne pas confondre avec l'action de G sur A)*

On dira que deux cocycles a et b sont cohomologues *si il existe $a \in A$ tel que $b_s = a^{-1}.a_s.s(a)$ pour tout $s \in G$.*

On démontre sans difficulté la proposition suivante.

Proposition 5.1. *La relation "être cohomologue" est une relation d'équivalence sur l'ensemble des cocycles.*

On peut alors construire l'ensemble quotient noté $H^1(G, A)$, dont on mettra en avant la classe d'équivalence du cocycle identité. On parle donc d'ensemble pointé, ce qui permet donc de définir le noyau d'un morphisme d'ensemble pointé (l'image réciproque du point privilégié) et donc de suites exactes. On peut en outre remarquer que ce H^1 coïncide avec la notion habituelle quand A est abélien, on a seulement "oublié" la structure de groupe, pour ne se rappeler que de l'élément privilégié : le neutre.

Considérons un autre G-module non abélien B, et un morphisme de groupe $f : A \to B$, qui commute à l'action de G. On définit alors des applications :

$$\begin{aligned} f_0 &: H^0(G, A) \to H^0(G, B) \quad \text{morphisme de groupes} \\ f_1 &: H^1(G, A) \to H^1(G, B) \quad \text{morphisme d'ensembles pointés} \end{aligned}$$

Où f_0 est simplement la restriction de f à A^G, il est facile de remarquer que l'image de f_0 est alors dans B^G.

Et où f_1 est construite en remarquant que si $\sigma : G \to A$ est un cocycle de A alors $f \circ \sigma$... un cocycle de B. Cette correspondance passe évidement au quotient par les propriétés de f, qui envoi la classe de l'identité de A sur celle de B.

L'objectif de cette partie est de pouvoir, à partir d'une suite exacte de G-modules non abéliens :

$$1 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 1 \tag{5.1}$$

Construire une suite exacte sur les ensembles pointés cohomologiques :

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

comme dans le cas abélien. Pour y parvenir nous verrons que nous sommes contraint d'imposer que A soit contenu dans le centre de B pour aller jusqu'au $H^2(G, A)$ (ce qui nous intéresse, le groupe $Br(k)$ étant un H^2).

Proposition 5.2. *On a un opérateur de cobord :*

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

Démonstration. On se donne $c \in C^G$. Par surjectivité de p, il existe $b \in B$ tel que $p(b) = c$. Or on remarque que pour $s \in G$:

$$p(b^{-1}.s(b)) = p(b^{-1}).p(s(b)) = p(b)^{-1}.s(p(b)) = c^{-1}.c = 1$$

Donc $b^{-1}.s(b) \in A$ par exactitude de la suite (5.1). On a ainsi définie une application :

$$\begin{aligned} a : G &\to A \\ s &\mapsto b^{-1}.s(b) \end{aligned}$$

d'une part il s'agit de voir que a est un cocycle de A. En effet :

$$\begin{aligned} a_{st} = b^{-1}.st(b) =& b^{-1}.s(t(b)) \\ =& b^{-1}.s(b).s(b^{-1}.t(b)) \\ =& a_s.s(a_t) \end{aligned}$$

D'autre part pour avoir la "bonne" définition de a dans $H^1(G, A)$, il faut vérifier que changer b, l'antécédent de c par p, équivaut à remplacer a par un cocycle cohomologue. Et en effet si $p(b) = p(b') = c$, on a comme précédemment un $a_0 \in A$ tel que $b' = b.a_0$. Alors si on note a' le cocycle associé à b' :

$$\begin{aligned} a'_s = b'^{-1}s(b') =& a_0^{-1}b^{-1}s(b)s(a_0) \\ =& a_0^{-1}a_s s(a_0) \end{aligned}$$

D'où a' et a sont cohomologues. Aisni δ envoie $c \in H^0(G, C)$ sur la classe de a est bien définie. □

On supposera connue la caractérisation du H^2 au moyen de cochaînes, c'est à dire qu'un 2-cocycle peut être vu comme une application $f : G \times G \to A$ vérifiant pour $u, s, t \in G$:

$$s(f(t, u)) = f(st, u)f(s, tu)^{-1}f(s, t)$$

Il s'agit en fait de trouver une "bonne" résolution injective pour calculer les H^n dans la définition du foncteur dérivé, en un sens précisé en annexe.

Proposition 5.3. *Si on suppose que A est contenue dans le centre de B. Il est alors abélien et nous pouvons considérer son $H^2(G, A)$ usuel, en oubliant sa structure de groupe au profit de sa structure d'ensemble pointé en le neutre. On a un opérateur de cobord :*

$$\Delta : H^1(G, C) \to H^2(G, A)$$

Démonstration. La démonstration complète est dans [Ser] page 132. Donnons tout de même l'expression de Δ. Si c est un cocycle de C, on a pour tout $s \in G$ un $b_s \in B$ tel que $p(b_s) = c_s$. Comme c est un cocycle et comme (5.1) est exacte, on a $b_{st}^{-1}b_s.s(b_t) \in A$. On définit alors

$$a : (s, t) \mapsto b_{st}^{-1}b_s.s(b_t)$$

On vérifie alors que c'est un 2-cocycle et que remplacer c par c' qui lui est cohomologue, ne change pas la classe de a dans $H^2(G, A)$. Cette application faisant alors correspondre la classe de c à la classe de a est le Δ cherché.

□

Nous allons voir que ces opérateurs de cobord permettent de créer la suite exacte de cohomologie non abélienne voulue.

Proposition 5.4. *Si on suppose que A est contenue dans le centre de B, dans la suite exacte* (5.1)*, alors la suite d'ensembles pointé suivante est exacte :*

$$1 \longrightarrow H^0(G,A) \xrightarrow{i_0} H^0(G,B) \xrightarrow{p_0} H^0(G,C) \xrightarrow{\delta} H^1(G,A) \xrightarrow{i_1} H^1(G,B) \xrightarrow{p_1} H^1(G,C) \xrightarrow{\Delta} H^2(G,A)$$

Démonstration. [Ser] page 133 □

5.2 Exemple de descente galoisienne

Dans tout ce chapitre on note k un corps, et K/k une extension galoisienne de dimension finie de groupe de Galois G. On fixe également V un k-espace vectoriel et $x \in \bigotimes^p V \otimes \bigotimes^q V^*$ où V^* est le dual de V.

Nous dirons donc que deux tels couples (V,x) et (V',x') sont k-isomorphes quand on a un isomorphisme de k-espace $f : V \to V'$ tel que $f(x) = x'$.

Définition 5.3. *Pour (V',x') un couple comme précédemment. On note V'_K l'extension des scalaires $V' \otimes_k K$, et x'_K l'élément correspondant.*
On dira alors que (V',x') et (V,x) deviennent K-isomorphes si les (V_K,x_K) et (V'_K,x'_K) sont K-isomorphes. On notera alors

$$E(K/k)$$

l'ensemble des classes prisent à k-isomorphismes près de couples (V',x') qui deviennent K-isomorphes à (V,x).

L'objectif est de trouver le bon angle pour voir $E(K/k)$ comme un H^1. Dans la suite nous notons $A_K = Aut_K(V_K,x_K)$ le groupe des K-automorphismes. C'est ce dernier que nous allons munir d'une structure de "G-module" non abélien.

Proposition 5.5. *Le groupe G agit sur A_K.*

Démonstration. On fait d'abord agir G sur V_K par :

$$\forall g \in G \quad g.(v \otimes \lambda) = v \otimes g(\lambda)$$

et en prolongeant par additivité. Ensuite pour $f \in A_K$ on pose :

$$\forall g \in G\,, w \in V_K \quad g.f(x) = g.(f(g^{-1}.w))$$

C'est à dire

$$\forall g \in G \quad g.f = g \circ f \circ g^{-1}$$

en ayant implicitement étendu g à V_K entier comme précédemment. □

On peut ainsi considérer $H^1(G,A_K)$. Construisons la bijection cherchée. On se donne pour cela $(V',x') \in E(K/k)$ et $f : V_K \to V'_K$ l'isomorphisme associé. On définit alors, pour $g \in G$:

$$p_g = f^{-1} \circ g.f = f^{-1} \circ g \circ f \circ g^{-1}$$

Proposition 5.6. *L'application $p : g \mapsto p_g$ est un 1-cocycle*

Démonstration. Nous utiliserons abondamment le principe du calcul cohomologique à l'aide de cochaînes, dans le cas non abélien (section précédente de l'annexe). On a par définition, d'une part :

$$p_{g_1g_2} = f^{-1} \circ g_1 \circ g_2 \circ f \circ g_2^{-1} \circ g_1^{-1}$$

Et d'autre part :

$$g_1.p_{g_2} = g_1 \circ f^{-1} \circ g_2 \circ f \circ g_2^{-1} \circ g_1^{-1}$$
$$p_{g_1} = f^{-1} \circ g_1 \circ f \circ g_1^{-1}$$

D'où l'égalité :

$$p_{g_1g_2} = p_{g_1} \circ g_1.p_{g_2}$$

Qui permet de conclure. □

Ainsi on peut considérer la classe de p dans $H^1(G, A_K)$, et la propriété suivante nous assure que nous pouvons le faire sans ambiguïté.

Proposition 5.7. *La classe de p dans $H^1(G, A_K)$ ne dépend pas de l'isomorphisme $f : V_K \to V'_K$ choisi au départ.*

Démonstration. En effet si f et f' sont deux tels isomorphismes, on note $p : g \mapsto f^{-1} \circ g.f$ et $q : g \mapsto f'^{-1} \circ g.f'$. On remarque en outre que $f \circ f'^{-1} \in A_K$ et on note a cet élément. On a alors :

$$\begin{aligned} q_g &= f'^{-1} \circ g \circ f' \circ g^{-1} \\ &= a^{-1} \circ f^{-1} \circ g \circ f \circ a \circ g^{-1} \\ &= a^{-1} \circ p_g \circ g \circ a \circ g^{-1} \\ &= a^{-1} \circ p_g \circ g.(a) \end{aligned}$$

Ainsi q et p sont cohomologues, et donc appartiennent à la même classe dans $H^1(G, A_K)$. □

Définition 5.4. *On peut alors définir proprement l'application suivante :*

$$\begin{aligned} \theta : \ & E(K/k) \to H^1(G, A_K) \\ & (V', x') \mapsto p \end{aligned}$$

Avec p comme précédemment.

On en arrive à l'objectif principal de cette section :

Théorème 5.1. *L'application θ est une bijection de $E(K/k)$ dans $H^1(G, A_K)$*

Démonstration. [Ser] page 161. Commençons par l'injectivité. Si (V'_1, x'_1) et (V'_1, x'_1) s'envoient sur le même p. On note pour $i \in \{1, 2\}$ le K-isomorphisme correspondant :

$$f_i : V \otimes_k K \longrightarrow V'_1 \otimes_k K$$

Alors par hypothèse, pour tout $s \in G$ on a :

$$f_1^{-1} \circ s(f_1) = f_2^{-1} \circ s(f_2)$$

et donc

$$f_2 f_1^{-1} = s(f_2 f_1^{-1})$$

Ainsi G fixe le K-isomorphisme $f_2 f_1^{-1}$. Donc comme K/k est galoisienne, on sait que les points fixes de l'actions de G sont les éléments de k. Ainsi $f_2 f_1^{-1}$ induit un k-isomorphisme entre (V'_1, x'_1) et (V'_1, x'_1).

Pour la surjectivité, prenons a un 1-cocycle de A_k. Comme $A_k \subset GL(V_K)$, et que le théorème de HIlbert (2.8) nous assure que $H^1(G, GL(V_K)) = 1$, alors il existe $f \in A_K$ tel que :

$$\forall s \in G \ \ a_s = f^{-1} \circ s(f)$$

On étend alors f linéairement à l'algèbre tensorielle de V_K, et posons $x' = f(x)$. Alors x' appartient en fait bien à l'algèbre tensorielle sur k de V, en effet pour $s \in G$:

$$\begin{aligned} s(x') =& s(f(x)) = s(f)(s(x)) \\ =& s(f)(x) \qquad \text{car } x \in \bigotimes^p V \otimes \bigotimes^q V^* \ \text{ comme } k\text{-espace vectoriel} \\ =& f \circ a_s(x) = f(x) \\ =& x' \end{aligned}$$

Donc x' est invariant par G. On peut ainsi affirmer que (V, x') appartient à $E(K/k)$ et que son image par θ est bien la classe de a par construction. □

5.3 Calcul cohomologique au moyen de cochaînes

Nous allons ici donner une méthode pour calculer les $H^i(G, A)$ en petite dimension. Pour cela nous allons nous appuyer sur le théorème (2.6), qui permet de construire les H^i à partir d'une résolution projective de $\mathbb{Z}$. Nous ne donnerons pas les preuves, et renvoyons à [Har] page 23 pour les détails.

Comme déjà mentionner, le point de vu projectif peut être plus simple à manipuler, car un G-module libre est projectif. Mettons en oeuvre cette idée.

Pour $i \in \mathbb{N}$ on note E_i l'ensemble des $(i+1)$-uplets $(g_0, \ldots, g_i)$ d'éléments de G. On considère alors L_i le $\mathbb{Z}$-module libre de base E_i. On fait agir G sur L_i par translation :

$$s.(g_0, \ldots, g_i) = (sg_0, \ldots, sg_i)$$

Proposition 5.8. *Les L_i sont des $\mathbb{Z}[G]$-modules libres (donc projectifs)*

Et plus précisément si on note $d_0 : L_0 \to \mathbb{Z}$ constant à 1, et pour $i > 0$, $d_i : L_i \to L_{i-1}$ les morphismes de G-modules :

$$d_i(g_0, \ldots, g_i) = \sum_{j=0}^{i} (-1)^j (g_0, \ldots, g_{j-1}, g_{j+1}, \ldots, g_i)$$

on a la proposition suivante :

Proposition 5.9. *La suite*

$$\ldots \longrightarrow L_2 \xrightarrow{d_2} L_1 \xrightarrow{d_1} L_0 \xrightarrow{d_0} \mathbb{Z} \longrightarrow 0$$

est exacte, et donc est une résolution projective de $\mathbb{Z}$ par des $\mathbb{Z}[G]$.

Soit maintenant A un G-module noté additivement. Notons $K_i = Hom_G(L_i, A)$, et on observe alors qu'un élément de K^i s'identifie à une fonction $f : G^i \to A$ telle que :

$$s.f(g_0, \ldots, g_i) = f(sg_0, \ldots, sg_i)$$

Le théorème (2.6) nous dis que les $H^i(G, A)$ sont alors les groupes de cohomologie du complexe :

$$0 \to K^0 \to K^1 \to \ldots$$

Et que les cobords $d^i : K^i \to K^{i+1}$ sont donnés par, pour $f \in K^i$:

$$\begin{aligned} d^i(f)(g_0, \ldots, g_{i+1}) =& g_i f(g_1, \ldots, g_{i+1}) \\ &+ \sum_{j=1}^{i} (-1)^j f(g_0, \ldots, g_{j-1}, g_j g_{j+1}, g_{j+2}, \ldots, g_{i+1}) + (-1)^{i+1} f(g_0, \ldots, g_i) \end{aligned}$$

Ainsi un 1-cocycle est une application $f : G \to A$ telle que :

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

Un 1-cobord est donc un 1-cocycle dans l'image de d^0, donc de la forme $g \mapsto g.a - a$ pour un $a \in A$.

Enfin, un 2-cocycle est une application $f : G \times G \to A$ telle que

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

Références

[Har] David Harari. *Cohomologie galoisienne et théorie du corps de classes*. CNRS.

[Lan] Serge Lang. *Algebra*. Springer.

[PG04] T. Szamuely P. Gille. *Central Simple Algebras and Galois Cohomology*. Cambridge Studies in advanced Mathematics, 2004.

[Ser] Jean-Pierre Serre. *Corps locaux*. Hermann.

[Wei] Charles.A Weibel. *An introduction to homological algebra*. Cambridge university press.