Introduction à la cohomologie galoisienne

Pierre Marry et Philippe Durand

novembre 2002

1 Introduction

Le but de ces exposés est d'introduire à l'occasion du seminaire du département de mathématique du CNAM sur la théorie de Galois quelques éléments de Théorie cohomologique qui doivent permettre de s'interesser aux propriétés topologiques des extensions galoisiennes infinies. Un cas particulier interessant motivant cette étude est l'anneau des entiers p-adiques qui repésente un cas particulier d'extensions galoisiennes infinies.

Le plan sera le suivant:

1. Notions d'algèbre Homologique
2. Homologie simpliciale et cohomologie simpliciale.
3. Cohomologie des groupes.
4. Limite projective de groupes, injective de modules.
5. Extensions galoisiennes finie et infinie de corps.
6. Groupes profinis et groupes de cohomologies associés.

2 Algèbre Homologique

2.1 Complexes, suites exactes

Définition. On appelle complexe $C.$ de $R-modules$ la famille $\{C_n\}_{n\in Z}$ avec

$$... \longrightarrow C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} C_{n-2} ...$$

et $\forall n \in Z$, $\partial_{n-1} \circ \partial_n = 0$

On a donné une version homologique de cette définition, il existe de même une version cohomologique:

On appelle complexe cohomologique $C^{\cdot}$ de $R-modules$ la famille $\{C^n\}_{n\in Z}$ avec

$... \longrightarrow C^{n-2} \overset{\delta^{n-2}}{\longrightarrow} C^{n-1} \overset{\delta^{n-1}}{\longrightarrow} C^n ...$

et $\forall n \in Z$, $\delta^n \circ \delta^{n-1} = 0$

On prend aussi en considération dans cette definition le cas des groupe abeliens en prenant pour l'anneau R l'ensemble Z.

Définition. On appelle suite exacte un complexe verifiant:

$... \longrightarrow X_{n-2} \overset{f_{n-2}}{\longrightarrow} X_{n-1} \overset{f_{n-1}}{\longrightarrow} X_n ...$

$\forall n \in Z, Kerf_{n-1} = Imf_{n-2}$

On appelle suite exacte courte:

$0 \longrightarrow X \overset{f}{\longrightarrow} Y \overset{g}{\longrightarrow} Z \longrightarrow 0$

$Kerg = Imf$

Exemple: Si $f$est un morphisme entre les $R-modules$ M et N on a les deux suites exactes:

$0 \longrightarrow Kerf \overset{i}{\longrightarrow} M \overset{\pi}{\longrightarrow} Coimf \longrightarrow 0$

$0 \longrightarrow Imf \overset{i}{\longrightarrow} N \overset{\pi}{\longrightarrow} Cokerf \longrightarrow 0$

avec $Cokerf = N/Imf$

$Coimf = M/Kerf$

En particulier si M et N sont des espaces vectoriels :

$M = Kerf \oplus Cokerf$ et $N = Imf \oplus Coimf$

On dit que la suite exacte "split", c'est faux pour les modules en général : existence d'une torsion. Voici deux exemples simples :

$0 \longrightarrow Z \overset{\times p}{\longrightarrow} Z \overset{\pi}{\longrightarrow} Z/pZ \longrightarrow 0$

$0 \longrightarrow Z/pZ \overset{\times q}{\longrightarrow} Z/pqZ \overset{\pi}{\longrightarrow} Z/qZ \longrightarrow 0$

Définition. $... \longrightarrow X_{n-2} \stackrel{f_{n-2}}{\longrightarrow} X_{n-1} \stackrel{f_{n-1}}{\longrightarrow} X_n ...$

On note $H^n(X.) = Kerf_n/Imf_{n-1}$

Ce quotient mesure le defaut d'exactitude du complexe c'est à dire la presence de (co)homologie.

Théorème. Etant donné un complexe $X.$ il existe un invariant noté $\chi(X.)$. C'est la caractèristique d'Euler Poincaré du complexe:

$\chi(X.) = \sum(-1)^i dimX_i = \sum(-1)^i dimH_i(X.)$

Exercice: que retrouve t'on quand on considère le complexe issue de la suite exacte courte vue ci dessus dans le cas ou les modules sont des espaces vectoriels :

$\longrightarrow Kerf \stackrel{i}{\longrightarrow} M \stackrel{\pi}{\longrightarrow} M/kerf \longrightarrow 0$

On rappelle que $M/kerf \simeq Imf$

2.2 Exemple : Cohomologie de de Rham sur un ouvert de R^2 ou une surface

Si U est un ouvert de R^2 On a le complexe ci dessous:

$0 \longrightarrow \mathcal{C}^O(U) \stackrel{d}{\longrightarrow} \mathcal{C}^1(U) \stackrel{d}{\longrightarrow} \mathcal{C}^2(U) \longrightarrow 0$

$\mathcal{C}^O(U)$ represente les fonctions continues sur l'ouvert U

$\mathcal{C}^1(U)$: les formes différentielles continues sur l'ouvert U de degré 1.

$\mathcal{C}^2(U)$: les formes différentielles continues sur l'ouvert U de degré 2.

Si U est un ouvert etoilé il est bien connu que toute forme différentielle fermée est exacte autrement dit les groupes de cohomologies pour $n \geq 1$ sont tous nul.

d'autre part $H^O(\mathcal{C}^\cdot(U)) = ker\ d$

Donc ce groupe de cohomologie donne les fonctions constantes:$H^O(\mathcal{C}^\cdot(U)) \simeq R$

Remarque: Si M est une variété elle peut être recouverte par des ouverts (de cartes)la cohomologie peut être calculée à partir du complexe de Cech dont une forme primaire est la suite exacte de Mayer Vietoris:

si $M = U \bigcup V$. Posons pour simplifier: $H^n(\mathcal{C}^{\cdot}(U)) = H^n(U)$, on a la longue suite exacte:

$$... \longrightarrow H^k(U) \bigoplus H^k((V) \longrightarrow H^k(U \bigcap V) \xrightarrow{\partial} H^{k+1}(U \bigcup V) \longrightarrow$$

$$H^{k+1}(U) \bigoplus H^{k+1}(V) \longrightarrow H^{k+1}(U \bigcap V) \longrightarrow ...$$

3 Homologie simpliciale, cohomologie simpliciale

Le materiel développé dans cette section c'est considerablement developpé. L'idée de départ est l'utilisation d'un complexe fabriqué à partir des polyèdres de R^n(avec eventuellement n infini).On s'intéresse à la triangulation de ces polyèdres ce qui debouche sur la notion de simplexe . On note K l'ensemble des simplexes orientés (ensemble de faces du polyèdre). A partir de K, On fabrique le complexe $\mathcal{C}_{\cdot}(K)$ dans lequel $\mathcal{C}_n(K)$ désigne le groupe abelien libre (donc un $Z - module$) engendré par les n-simplexes orientés. Tout cela s'insert dans la théorie générale des ensemble simpliciaux. qui est le cadre naturel (et théorique) pour définir la cohomologie des groupes, mais il faudrait alors plus d'outils d'algèbre homologique: resolutions,...etc . On peut comprendre les idées fondamentales en restant au niveau du complexe défini plus haut.

3.1 Homologie simpliciale

On considère donc le complexe $\mathcal{C}_{\cdot}(K)$ associé aux n simplexes:

$$... \longrightarrow \mathcal{C}_n(K) \xrightarrow{\partial_n} \mathcal{C}_{n-1}(K) \xrightarrow{\partial_{n-1}} \mathcal{C}_{n-2}(K)... \xrightarrow{\partial_0} \mathcal{C}_0(K) \longrightarrow O$$

Soit $\sigma_r = (p_0, p_1, ...p_r)$, un r-simplexe orienté

$$\partial_r \sigma_r = \sum_{i=1}^{r} (-1)^i (p_0, p_1, ..., \hat{p}_i, ...p_r).$$

∂_r vérifie les bonnes propriétés.

3.2 Cohomologie simpliciale

Par dualité on peut definir a partir des éléments du paragraphe precedent la cohomologie simpliciale:

Considerons l'ensemble $\mathcal{C}^n(K,R)$ des applications de $\mathcal{C}_n(K)$ dans R On défini alors le complexe $\mathcal{C}^\cdot(K,R)$ en sens inverse:

$$0 \longrightarrow \mathcal{C}^0(K,R) \xrightarrow{d} \mathcal{C}^1(K,R) \xrightarrow{d} ...\mathcal{C}^{n-1}(K,R) \xrightarrow{d} \mathcal{C}^n(K,R) \longrightarrow ...$$

Soit $\sigma_r = (p_0, p_1, ...p_r)$, un r-simplexe orienté

$$\langle df, \sigma_r \rangle = \langle f, \partial_r \sigma_r \rangle = \sum_{i=1}^{r} (-1)^i f(p_0, p_1, ..., \hat{p}_i, ...p_r).$$

par linéarité. Cette dernière expression n'est pas sans rappeler la formule de Stoke...:

$$\int_{(p_0,p_1,...p_r)} df = \int_{\partial_r(p_0,p_1,...p_r)} f$$

On peut à partir des outils ainsi definis mais ce n'est pas l'objet du présent exposé définir l'homologie (et la cohomologie) singulière sur une variété ainsi que la cohomologie de de Rham

4 Cohomologie des groupes

Ce paragraphe est la traduction du précedent dans le cadre de la théorie des groupes. On s'interesse maintenant à la categorie des groupes topologiques G et ses representations dans des G-modules topologiques A. Les sommets du simplexe K de R^n sont des élément du groupe G, à partir des simplexes de G on construit l'homologie des groupes et quand on prend sa representation dans un G-module A la cohomologie des groupes qui nous interesse ici. Il est utile à ce point de l'exposé de rappeler quelques définitions.

4.1 Groupes topologiques, G-modules topologiques

Groupe topologique

Un groupe topologique (G,.) est un groupe muni d'une topologie rendant au moins continue le produit et l'inverse.

En particulier les translation à droite et à gauche sont continues. Il en resulte que les ouverts contenant a sont les translatés des ouverts contenant e élément neutre du groupe.

exemples R^n, tout groupe de Lie sont des groupes topololologiques.

G-module topologique

Un G-module A est un ensemble verifiant les axiomes ci-dessous:

(A,+) est un groupe commutatif;

Si on note g un élément quelconque du groupe, a, b quelconques dans l'algèbre:

g.(a+b) = g.a + g.b

g'.(g.a) = (g'.g).a

e.a = a

Si la loi externe définie est continue le module est topologique.

4.2 Cohomologie des groupes

Etant donné un groupe topologique G et un module topologique A. Considerons l'ensemble $\mathcal{F}^n(G,A)$ des applications de G^n dans A.

On définit alors le complexe $\mathcal{F}^{\cdot}(G,A)$:

$0 \longrightarrow \mathcal{F}^0(G,A) \xrightarrow{d} \mathcal{F}^1(G,A) \xrightarrow{d} ... \xrightarrow{d} \mathcal{F}^{n-1}(G,A) \xrightarrow{d} \mathcal{F}^n(G,A) \longrightarrow ...$

Soit $(g_0, g_1, ..., g_r)$, un élément de G^r

$$\mathrm{df}((g_0, g_1, ..., g_r)) = f(\partial_r(g_0, g_1, ..., g_r)) = \sum_{i=1}^{r}(-1)^i f(g_0, g_1, ..., \hat{g}_i, ...g_r).$$

Remarque : On montre sans difficultées que $\mathcal{F}^0(G,A) \simeq A$

Proposition: Le complexe défini ci-dessus est exact.

En effet il suffit de définir $h^n : \mathcal{F}^{n+1}(G,A) \longrightarrow \mathcal{F}^n(G,A)$ par:

$h^n(f)(g_0, g_1, ..., g_{n-1}) = f(1, g_0, g_1, ..., g_{n-1})$

et montrer l'identité: $d^n h^n + h^{n+1} d^{n+1} = 1$ (faire le calcul)

si $d^{n+1} f = 0 (f \in Ker d^{n+1})$ alors $d^n h^n f = f (f \in Im d^n)$

l'autre inclusion étant acquise par définition d'un complexe.

Complexe homogène

Il est utile de définir le complexe des fonctions homogènes de n+1 variables: $\mathcal{C}^n(G,A)$

$\mathcal{C}^n(G,A) = \{f \in \mathcal{F}^{n+1}(G,A), f(g.g_0,...,g.g_n) = g.f(g_0,...,g_n)\}$

Théorème . Les deux complexes précédents $\mathcal{C}^n(G,A)$, $\mathcal{F}^n(G,A)$ sont en bijection.

En effet, notons φ dans $\mathcal{F}^n(G,A)$ et fabriquons son image f_φ dans $\mathcal{C}^n(G,A)$

on a : $f_\varphi(g_0,...,g_n) = g_0.f_\varphi(1, g_0^{-1}.g_1,...,g_0^{-1}.g_n)$

Donc $f_\varphi(g_0,...,g_n) = g_0.\varphi(g_0^{-1}.g_1,...,g_0^{-1}.g_n)$

Réciproquement,donnons f dans $\mathcal{C}^n(G,A)$, l'image réciproque est donnée par:

$\varphi_f(g_1,...g_n) = f(1, g_1, g_1.g_2,...,g_1.g_2...g_n)$

Foncteur cohomologique

Un foncteur cohomologique $\mathcal{S}$ d'une catégorie $\mathcal{C}$ dans une catégorie $\mathcal{C}'$ est la donnée:

(1) D'une suite : $\mathcal{S}^0, \mathcal{S}^1, \mathcal{S}^2, ...$

(2) Pour toute suite exacte dans $\mathcal{C}$:

$0 \longrightarrow A \xrightarrow{u} B \xrightarrow{v} C \longrightarrow 0$

d'une suite de cobords ∂_n: $\mathcal{S}^n(C) \longrightarrow \mathcal{S}^{n+1}(A)$

permettant de définir une longue suite exacte de cohomologie:

$0 \longrightarrow \mathcal{S}^0(A) \longrightarrow \mathcal{S}^0(B) \longrightarrow \mathcal{S}^0(C) \xrightarrow{\partial_0} \mathcal{S}^1(A) \longrightarrow ...$

$\longrightarrow \mathcal{S}^n(A) \longrightarrow \mathcal{S}^n(B) \longrightarrow \mathcal{S}^n(C) \xrightarrow{\partial_n} \mathcal{S}^{n+1}(A) \longrightarrow ...$

(3).Pour tout diagramme commutatif à lignes exactes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

d'un diagramme commutatif de même style en cohomologie:

$$\begin{array}{ccc} \mathcal{S}^n(C) & \longrightarrow & \mathcal{S}^{n+1}(A) \\ \downarrow & & \downarrow \\ \mathcal{S}^n(C') & \longrightarrow & \mathcal{S}^{n+1}(A') \end{array}$$

exemple: Les foncteurs classiques de cohomologie (defaut d'exactitude de complexes) permettent à partir d'une suite exacte courte de complexes de fabriquer de longues suites exactes et sont donc trivialement des foncteurs cohomologiques.

G-modules induits

Soit G un groupe topologique, X un groupe abelien eventuellement discret. On appelle G-module induit l'ensemble:

$\mathcal{M}_G(X) = \{f : G \to X / s.f(g) = f(g.s)\}$

Un résultat important est qu'il ne peut y avoir de cohomologie avec de tels modules.

Théorème . Soit $\mathcal{S}$ un foncteur cohomologique vérifiant

(1) $\mathcal{S}^0(A) = A^G$ (éléments invariants par G)

(2) Pour tout G-module induit, $\mathcal{S}^n(A) = 0$

Alors, l'homologie d'un G-module quelconque A est: $\mathcal{S}^n(A) = H^n(G, A)$

4.3 Calcul de la cohomologie du groupe cyclique

Soit G le groupe cyclique d'ordre n, s sont générateur, A un G-module.

Soit les deux homomorphismes N, D définis ci-dessous

$Na = a + sa + ... + s^{n-1}a$, $Da = sa - a$

On verifie que $D \circ N = N \circ D = 0$.

On a alors le complexe:

$0 \longrightarrow A \xrightarrow{D} A \xrightarrow{N} A \xrightarrow{D} A \xrightarrow{N} ...$

Théorème .Notons $\mathcal{S}^i(A)$ l'homologie de ce complexe. On verifie que $\mathcal{S}$ est un foncteur cohomologique:

-$\mathcal{S}^0(A) = A^G$

- Pour tout module induit $A = \mathcal{M}_G(X)$, $\mathcal{S}^n(A) = 0$

Le premier point est évident, montrons le second.

(1) n pair: soit f une fonction de $A = \mathcal{M}_G(X)$ si $Df = 0$, ce qui signifie que f est la fonction constante $f(x) = a$. Il faut alors trouver une fonction h du même ensemble telle que $Nh = f$.

on a alors: $Nh(g) = h(g) + sh(g) + ... + s^{n-1}h(g) = a$

et comme $\mathrm{M}_G(X)$ est un module induit:

Il vient : $Nh(g) = h(g) + h(gs) + ... + h(gs^{n-1}) = a$

Il suffit donc de prendre $h(g) = a, h(gs^i) = 0$ pour $i \neq 0$

(2) Le cas impair est laissé en exercice.

Ce dernier resultat donne un procèd de calcul des groupes de cohomologie des groupes cycliques:

Exercices d'applications :

(a) Determiner dans le cas $A = C$ la cohomologie du groupe des racines de l'unité.

(b) Même question pour le groupe des permutations de n variables indépendantes sur Z en prenant $A = Z(a_1, ...a_n)$

4.4 Limite inductive, limite projective d'ensembles

Définition Un système inductif d'ensembles E_i indexés par $(I, \leq)$ est une famille: $(E_i)_{i\in I}$ et d'applications: $u_{i,j} : E_i \to E_j$ si $i \leq j$ avec

$u_{i,i} = id_{E_i}, u_{j,k} \circ u_{i,j} = u_{i,k}$ si $i \leq j \leq k$

Etant donné un ensemble E, des morphismes $u_i : E_i \to E$ satisfaisant la propriété universelle:

pour tout ensemble F et toute famille de morphismes $f_i : E_i \to F$ vérifiant $f_i = f_j \circ u_{i,j}, i \leq j$,il existe un unique morphisme f :$E \to F$ avec $f_i = f \circ u_i$.

Un tel E existe, est unique. On dit que E est la limite inductive des E_i on note:

$$E = \underset{\rightarrow}{lim} \; E_i$$

Définition Un système projectif d'ensembles E_i indexés par $(I, \leq)$ est une famille: $(E_i)_{i \in I}$ et d'applications: $p_{i,j} : E_j \rightarrow E_i$ si $i \leq j$ avec

$p_{i,i} = id_{E_i}, p_{i,j} \circ p_{j,k} = p_{i,k}$ si $i \leq j \leq k$

Etant donné un ensemble E, des morphismes $p_i : E \rightarrow E_i$ satisfaisant une propriété universelle:

pour tout ensemble F et toute famille de morphismes $f_i : F \rightarrow E_i$ tel que $f_i = p_{i,j} \circ f_j$, $i \leq j$ il existe un unique morphisme f :$F \rightarrow E$ avec $f_i = p_i \circ f$. Un tel E existe on dit que E est la limite projective des E_i on note:

$$E = \underset{\leftarrow}{lim} \; E_i$$