Algèbre Commutative et Algèbre Homologique

Classe sino-française, USTC

Responsables du cours :
Prof. **Loic Merel**[1] et
Prof. **ZHANG Lei**[2]

D'après un polycopié de
CHEN Moqing

Février 2022 -Avril 2022

1. www.math.univ-paris13.fr/∼marchal/
2. sites.google.com/view/wensun-proba

Table des matières

Chapitre 1

Anneau de polynômes

1.1 Algèbre sur un anneau

Pour ce cours : anneau=anneau commutatif (sauf si on dit le contraire)

Soit A un anneau. Une $A-$algèbre est un $A-$module avec une application $A-$bilinéaire

$$B \times B \longrightarrow B \qquad (b_1, b_2) \mapsto b_1 \cdot b_2.$$

Cela donne une loi de composition, qu' on suppose associative (algèbre associative) et on suppose qu'il existe $1 \in B$ tel que $1 \cdot b = b \cdot 1 = b$ pour tout $b \in B$ (algèbre unitaire).

Pour ce cours : algèbre=algèbre associative unitaire.

Si $B' \subset B$, on dit que c'est une sous-algèbre de B si c'est un sous$-A-$module de B et $B \times B \to B$, $(b_1, b_2) \mapsto b_1 \cdot b_2$ induit $B' \times B' \to B'$ et de plus $1 \in B'$.

Soit $X \subset B$. La sous-algèbre engendrée par X est la plus petite sous algèbre de B contenant A et X.

Remarques 1.1.1. *Si B est une $A-$algèbre, on a vu morphisme d'anneau*

$$A \longrightarrow B$$
$$a \mapsto a \cdot 1.$$

"contenant A"=contenant l'image du morphisme.

On dit que B est une algèbre de type fini sur A si B est engendrée par un ensemble fini sur A. ($\neq$module de type fini). Pour k corps, $k[x]$ est une algèbre de type fini, mais pas un module de type fini.

Un monoïde est un ensemble M muni d'une loi de composition $M \times M \to M$ notée $\circ$ qui est associative et pour laquelle on a un élément neutre 1. On dit qu'il est commutatif si la loi est commutative.

Considérons $A[M] = \{M \to A, \textit{presquenulle}\}$. φ est presque nulle si $\{m \in M \mid \varphi(m) \neq 0\}$ est fini. Ici A est un anneau et M un monoïde commutatif. Pour $\varphi : M \to A$ presque nulle, on note $\sum_{m \in M} \varphi(m)[m]$ l'élément correspondant. $A[M]$ est une $A-$algèbre. C'est un $A-$module libre de base $([m])_{m \in M}$. La multiplication est donnée par $[m] \cdot [m'] \mapsto [m \cdot m']$ est par $A-$bilinéaire.

Pour $M = (\mathbb{N}, +)$. On pose $A[X] = A[\mathbb{N}]$ où X est l'élément $[\delta_1]$, où δ_1 est la fonction caractérestique de $1 \in \mathbb{N}$, $\delta_1(n) = 0$ si $n \neq 1$, $\delta_1 = 1$.

$A[X]$ est l'anneau des polynômes en une indéterminées à coefficients dans A.

Soit I un ensemble. On pose $\mathbb{N}^{(I)} = \{I \to \mathbb{N}\ \textit{presque nulle}\}$. C'est un monoïde commutatif. On pose $A[(X_i)_{i \in I}] = A[\mathbb{N}^{(I)}]$. C'est l'algèbre des polynômes à coefficients dans A en les indéterminées $(X_i)_{i \in I}$.

Pour $I = \{1, 2, \cdots, n\}$, on pose $A[\mathbb{N}^{(I)}] = A[X_1, \cdots, X_n]$. Ici, X_i est l'application $\mathbb{N}^{(I)} \to A$ qui à tout élément associe 0 sauf la fonction caractéristique de i ($\delta_i : I \to \mathbb{N}$ qui a $i \mapsto 1$, $j \mapsto 0$ si $j \neq i$) $X_i : \delta_i \mapsto 1$.

La $A-$algèbre $A[(X_i)_{i \in I}]$ a la propriété universelle suivante. Soit B une $A-$algèbre. Soit $(b_i)_{i \in I}$ une famille d'éléments de B. Il existe un unique morphisme de $A-$algèbres $A[(X_i)_{i \in I}] \to B$ tel que $X_i \mapsto b_i$ et pour $a \in A$ $a \mapsto a \cdot 1$. Ce morphisme s'appelle l'évaluation ou la spécialisation en $(b_i)_{i \in I}$.

On dit que B est engendré par $(b_i)_{i\in I}$ comme $A-$algèbre si ce morphisme est surjectif. C'est équivalent à dire que B est engendré par $\{b_i, i \in I\}$.

On dit que la famille $(b_i)_{i\in I}$ est algébriquement indépendante sur A, si ce morphisme est injectif. Ce morphisme de $A-$algèbre est un morphisme d'anneaux. Notons I son noyau. Si I est de type fini, on dit que B est de présentation finie sur A.

1.2 Anneaux noethériens

$$\begin{array}{ccc} k\ corps & \longrightarrow & A\ anneau \\ k-espace\ vectoriel & \longrightarrow & A-module \\ k-espace\ vectoriel & \longrightarrow & A-module \\ de\ dimension\ finie & & noethérien \end{array}$$

Une suite $(u_n)_{n\geq 0}$ est dite stationnaire s'il existe un entier $n_0 \geq 0$ tel que pour tout $n \geq n_0$, on a $u_n = u_{n_0}$.

Un anneau A est dit noethérien si toute suite croissante d'idéaux de A est stationnaire.

Proposition 1.2.1. *A est noéthérien si et seulement si tout idéal de A est de type fini sur A.*

Démonstration. Suppose A noethérien. Soit I un idéal de A. Montrons qu'il est de type fini. Soit $x_1 \in I$ et posons $I_1 = A_{x_1} \subset I$. S'il existe $x_2 = I - I_1$, posons $I_2 = Ax_1 + Ax_2$. On construit ainsi une suite croissante d'idéaux de A contenues dans I. On pose $I_{k+1} = I_k + Ax_{k+1}$ avec $x_{k+1} \in I - I_k$.

On a $I_k \subsetneq I_{k+1}$ donc la suite n'est pas stationnaire. Donc il existe k tel que $I = I_k$, ainsi que I est de type fini. Réciproquement, supposons que tout idéal de A est de type fini. Soit $(I_k)_{k\geq 0}$ une suite croissante d'ideaux de A. Posons $I = \cup_{k\geq 0} I_k$. C'est un idéal de A. Il est de type fini sur A. Soit X une partie génératrice finie. Il existe pour tout $x \in X$ k_x entier tel que $x \in I_{k_x}$. Posons $k = \max\{k_x, x \in X\}$ entier. On a $X \subset I_k$ car la suite est croissante. Donc $X \subset I_k \subset I_{k+1} \subset \cdots \subset I$, donc $I_k = I$. □

Proposition 1.2.2. *Soit A un anneau noethérien. Soit I un idéal de A. Alors A/I est un anneau noethérien.*

Démonstration. Soit $(J_k)_{k\geq 0}$ une suite croissante d'idéaux de A/I. Soit $\pi : A \to A/I$ la surjection canonique. Alors $(\pi^{-1}(J_k))_{k\geq 0}$ est une suite croissante d'idéaux de A. Elle est stationnaire car A est noethérien, Mais $J_k = \pi(\pi^{-1}(J_k))$. Donc $(J_k)_{k\geq 0}$ est une suite stationnaire. Donc A/I est noethérien. □

Quelques anneaux non noethériens

– $k[(X_i)_{i\in\mathbb{N}}]$ n'est pas noethérien pour k corps.

– $\overline{\mathbb{Z}} = \{x \in \mathbb{C} \mid x \textit{ entier algébrique}\}$ n'est pas noethérien car $(2^{\frac{1}{2^n}}\overline{\mathbb{Z}})_{n\geq 1}$ est une suite croissante d'idéaux.

– $\{f : \mathbb{R} \to \mathbb{R} \mid f \textit{ continue}\}$.

L'anneau $k[(X_i)_{i\in\mathbb{N}}]$ est un sous-anneau non noethérien du corps $\mathrm{Frac}(k[(X_i)_{i\in\mathbb{N}}]$ qui est noethérien.

Proposition 1.2.3. *Si A est un anneau principal, il est noethérien.*

Démonstration. Soit $(I_k)_{k\geq 0}$ une suite croissante d'idéaux de A. Posons $I = \cup_{k\geq 0} I_k$. C'est un idéal, forcément principal. Donc il existe $a \in A$ tel que $I = Aa$. Il existe k entier tek que $a \in I_k$. Donc on a

$$aA \subset I_k \subset I_{k+1} \subset \cdots \subset I = Aa.$$

Donc $I_k = I$. Donc la suite est stationnaire. □

L'anneau $k[(X_i)_{i\in\mathbb{N}}]$ est factoriel mais pas noethérien.

L'anneau $\mathbb{Z}[\sqrt{-5}]$ est noethérien mais pas factoriel. $\left(6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})\right)$

Proposition 1.2.4. *Si A est un anneau noethérien, tout élément est produit d'éléments irréductibles.*

Démonstration. Soit $a \in A$. Si a est réductible, il existe $a_1 \in A\backslash A^\times$, $b \in A\backslash A^\times$ tels que $a = a_1 b_1$, si a_1, b_1 sont irréductibles, c'est terminé. Sinon disons a_1 réductible, alors $a_1 = a_2 b_2$ avec $a_2, b_2 \in A\backslash A^\times$. Si a n'est pas produit d'irréductibles, il existe une suite $(a_k)_{k\geq 1} et (b_k)_{k\geq 1}$ tels que $a = a_k b_k a_{k-1} b_{k-1} \cdots b_1$ et $a_k, b_k \notin A\backslash A^\times$. On a $a_k | a_{k-1}$.

Donc la suite $(Aa_k)_{k\geq 1}$ est croissante strictement car $b_k \notin A^\times$. Donc c'est absurde car A est noethérien. □

Exemples 1.2.5. d'anneaux noethériens : $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, corps, $k[X]$ pour k corps, $\mathcal{O}_K$ =anneau des entiers d'un corps de nombres K.

Si A est un anneau factoriel, $A[X]$ est factoriel. (propriété héréditaire)

Théorème 1.2.6. *(de la base de Hilbert) Si A est un anneau noethérien, $A[X]$ est un anneau noethérien.*

Démonstration. Soit I un idéal de $A[X]$. Montrons qu'il est de type fini. Posons $B = \{b \in A \mid il\ existeP = bX^m + terme\ de\ degr < m\}$. C'est un idéal de A, car pour $b, b' \in B$ il existe $P = bX^m + \cdots$, $P' = b'X^{m'} + \cdots \in I$ avec $m \leq m'$ alors $X^{m'-m}P \in I$ et $X^{m'-m}P + P' = (b+b')X^{m'} + \cdots \in I$. Donc $b+b' \in B$. Pour $a \in A$, on a $aP = abX^m + \cdots$, donc $ab \in B$.

Comme A est noethérien, B est de type fini. Il existe $b_0, \cdots, b_{m-1} \in B$ tels que

$$B = Ab_0 + \cdots + Ab_{m-1}.$$

Il existe $P_0, \cdots, P_{m-1} \in I$ tels que

$$P_i = b_i X^{d_i} + \cdots$$

On pose $d = \max\{d_0, \cdots, d_{m-1}\}$. Soit k un entier≥ 1. Posons

$$B_k = \{\underbrace{b}_{\in 0} \in A \mid il\ existe\ P = bX^n + \cdots \in I\ avec\ n < k\}.$$

De même que B, B_k est un idéal de A comme A est noethérien, il existe $b_0^{(k)}, \cdots, b_{m_k-1}^{(k)}$ tels que

$$B_k = Ab_0^{(k)} + \cdots + Ab_{m_k-1}^{(k)}.$$

Il existe $P_0^{(k)}, \cdots, P_{m_k-1}^{(k)} \in I$ avec $P_i^{(k)} = b_i^{(k)} X^{n_k} + \cdots$.

Soit J =idéal engendré par $\{P_j P_i^{(k)} \mid 0 \leq j \leq m-1,\ 0 \leq k \leq d,\ 0 \leq i \leq m_k - 1\}$ (ensemble fini). On va montrer que $I = J$ (en donc I de type fini). On a $J \subset I$. Supposons $I \neq J$. Il existe $Q \in I - J$. Supposons Q de degré minimal. Posons $Q = qX^{d^\circ(Q)} + \cdots$. On considère deux cas : $d^\circ(Q) \geq d$ et $d^\circ(Q) < d$.

Si $d^\circ(Q) \geq d$, on a $q \in B$. On peut écrire $q = \sum_j \lambda_j b_j$ avec $\lambda_j \in A$, $P_j = b_j X^{d^\circ(P_j)} + \cdots$. Posons $Q_0 = \sum_j \lambda_j P_j X^{d^\circ(Q) - d^\circ(P_j)} \in I$ et même $Q_0 \in J$. On a $d^\circ(Q_0) = d^\circ(Q)$ et

$$\begin{aligned} Q_0 &= (\sum_j \lambda_j b_j) X^{d^\circ(Q)} + \cdots \\ &= qX^{d^\circ(Q)} + \cdots . \end{aligned}$$

Comme $Q \in I - J et Q_0 \in J$, on a $Q - Q_0 \in I - J$. Mais $Q - Q_0 = (qX^{d^\circ(Q)} + \cdots) - (qX^{d^\circ(Q)} + \cdots)$. Donc $d^\circ(Q - Q_0) < d^\circ(Q)$.

Absurde car Q est de degré minimal parmi les éléments de $I \backslash J$.

Il reste le cas où $d^\circ(Q) < d$. Si $d^\circ(Q) < d$, on pose de même $Q = qX^{d^\circ(Q)} + \cdots$. On a $q \in B_k$ et on pose $q = \sum_j \lambda_j b_j^{(k)}$ avec $\lambda_j \in A$. On pose

$$\begin{aligned} Q_0 &= \sum_j \lambda_j P_j^{(k)} X^{d^\circ(Q) - d^\circ(P_j^{(k)})} \\ &= \sum_j \lambda_j b_j^{(k)} X^{d^\circ(Q)} + \cdots \\ &= qX^{d^\circ(Q)} + \cdots \in J. \end{aligned}$$

On a $Q - Q_0 = (qX^{d^\circ(Q)} + \cdots) - (qX^{d^\circ(Q)} + \cdots) \in I - J$ car $Q \in I - J$. Donc $Q - Q_0 \in I - J$, $d^\circ(Q - Q_0) < d^\circ(Q)$ absurde.

Donc $I = J$. □

Corollaire 1.2.7. *Soit n un entier≥ 1, l'anneau $A[X_1, \cdots, X_n]$ est noethérien lorsque A est noethérien. (par exemple A est un corps)*

Démonstration. En effet, $A[X_1, \cdots, X_n] = A[X_1, \cdots, X_{n-1}][X_n]$ récurrence immédiate. □

Corollaire 1.2.8. *Toute algèbre de type fini B sur un anneau noethérien A est de présentation finie.*

Démonstration. En effet, $A[X_1, \cdots, X_n] \longrightarrow B$ surjective de noyau $I \subset A[X_1, \cdots, X_n]$ de type fini. □

1.3 Polynôme symétrique

Soit A un anneau. Soit n un entier≥ 1. Considérons $A[X_1, \cdots, X_n]$.
Posons $\mathfrak{S}_n =$ *groupe symtrique sur n lettres* et $\mathfrak{A}_n =$ *groupe alterné sur n lettres* $\subset \mathfrak{S}_n$.
$\mathfrak{S}_n$ agit sur $A[X_1, \cdots, X_n]$ par

$$(P(X_1, \cdots, X_n), \sigma) \mapsto P(X_{\sigma(1)}, \cdots, X_{\sigma(n)}) = \sigma(P)(X_1, \cdots, X_n)$$

On dit que $P \in A[X_1, \cdots, X_n]$ est du polynôme symétrique si $\sigma(P) = P$ pour tout $\sigma \in \mathfrak{S}_n$.

Exemples 1.3.1. Pour k entier≥ 0, on pose $\pi_k = \sum_{i=1}^{n} X_i^k$.

Pour k entier≥ 0, $k \leq n$, on pose

$$e_k = \sum_{1 \leq j_1 \leq \cdots \leq j_k \leq n} X_{j_1} \cdots X_{j_k}.$$

C'est le polynôme symétrique élémentaire de degré k. On a

$$e_0 = 1,\ e_1 = X_1 + \cdots + X_n,\ e_2 = \sum_{1 \leq i < j \leq n} X_i X_j, \cdots,\ e_n = X_1 \cdots X_n.$$

Si $k > n$, on pose $e_k = 0$.

Proposition 1.3.2. *(Formule de Viëte) On a*

$$\prod_{i=1}^{n} (T - X_i) = \sum_{k=0}^{n} (-1)^k e_k T^{n-k}$$

.

(relation entre les coefficients et les racines d'un polynôme)

Viëte (1540-1603)

$$\begin{array}{ccc} \textit{Racines d'un polynme} & \rightarrow & \textit{coefficients} \\ & \overset{?}{\leftarrow} & \end{array}$$

degré 3=formule de cardan
degré 4=résolvantes de Lagrange
degré 5=pas de formule (Abel)

Théorie générale : Galois (1811-1832).

Théorème 1.3.3. *Soit $P \in A[X_1, \cdots, X_n]^{\mathfrak{S}_n} = \{$Polynômes symétrique$\}$, il existe un unique polynôme $Q \in A[Y_1, \cdots, Y_n]$ tel que*

$$P(X_1, \cdots, X_n) = Q(e_1, \cdots, e_n).$$

Remarques 1.3.4.

1. *Comme Q unique, cela preuve que $e_1, \cdots, e_n$ sont algébriquement indépendants sur A.*

2. *On a un morphisme de A-algèbres*

$$\begin{aligned} A[Y_1, \cdots, Y_n] &\longrightarrow A[X_1, \cdots, X_n]^{\mathfrak{S}_n} \\ Q &\longmapsto Q(e_1, \cdots, e_n). \end{aligned}$$

3. *Le polynôme e_k sont homogènes de degré k.*

Démonstration. On peut supposer P homogène de degré d. Montrons l'existence de Q par une double récurrence sur d et n. Pour $n = 1$, OK. Un polynôme de $A[X_1, \cdots, X_n]$ est dit lacunaire s'il s'écrit

$$\sum_{\substack{\alpha_1, \cdots, \alpha_n \geq 0 \\ avec\ \alpha_1 \cdots \alpha_n = 0}} a_{\alpha_1, \cdots, \alpha_n} X_1^{\alpha_1} \cdots X_n^{\alpha_n} \qquad avec\ a_{\alpha_1, \cdots, \alpha_n} \in A.$$

Notons $\mathscr{L}$ l'ensemble des polynômes symétriques et lacunaires de $A[X_1, \cdots, X_n]$. □

Lemme 1.3.5. *L'application*

$$\begin{aligned} \mathscr{L} &\longrightarrow A[X_1, \cdots, X_{n-1}] \\ P &\longmapsto P(X_1, \cdots, X_{n-1}, 0) \end{aligned}$$

est injective.

Démonstration. Soit R dans le noyau. On a $R(X_1, \cdots, X_{n-1}, 0) = 0$. Donc il existe $P_1 \in A[X_1, \cdots, X_n]$ tel que $R = X_n R_1$. Comme R est symétrique, on a $R = \tau(R) = \tau(X_n)\tau(R_1)$ pour tout $\tau \in \mathfrak{S}_n$. Donc X_1 divise R pour tout $i \in \{1, \cdots, n\}$. Donc $X_1 \cdots X_n$ divise R.

Comme R est lacunaire, cela entraîne $R = 0$.

Tout polynôme symétrique s'écrit comme

$$(\textit{Polynôme lacunaire symétrique}) + X_1 \cdots X_n (\textit{Polynôme symétrique}).$$

En d'autres termes

$$A[X_1, \cdots, X_n]^{\mathfrak{S}_n} = \mathscr{L} \oplus X_1 \cdots X_n A[X_1, \cdots, X_n]^{\mathfrak{S}_n}.$$

(Somme directe de $A-$modules)

Revenons au théorème. Posons $P = P_0 + e_n P_1$ avec $P_0 \in \mathscr{L}$ et $P_1 \in A[X_1, \cdots, X_n]^{\mathfrak{S}_n}$. Posons

$$\widetilde{P}(X_1, \cdots, X_{n-1}) = P(X_1, \cdots, X_{n-1}, 0) = P_0(X_1, \cdots, X_{n-1}, 0) \in A[X_1, \cdots, X_{n-1}]^{\mathfrak{S}_{n-1}}.$$

Par hypothèse de récurrence, il existe $\widetilde{Q} \in A[Y_1, \cdots, Y_{n-1}]$ tel que

$$\widetilde{P}(X_1, \cdots, X_{n-1}) = \widetilde{Q}(\widetilde{e_1}, \cdots, \widetilde{e_{n-1}})$$

où $\widetilde{e_i}$ polynôme symétrique élémentaire de $A[X_1, \cdots, X_{n-1}]$. (il est obtenu en spécialement e_i en $X_n = 0$)

On pose $R(X_1, \cdots, X_n) = \widetilde{Q}(e_1, \cdots, e_{n-1}) \in A[X_1, \cdots, X_n]^{\mathfrak{S}_n}$. On a

$$\begin{aligned} R(X_1, \cdots, X_{n-1}, 0) &= \widetilde{Q}(\widetilde{e_1}, \cdots, \widetilde{e_{n-1}}) \\ &= \widetilde{P}(X_1, \cdots, X_{n-1}) \\ &= P(X_1, \cdots, X_{n-1}, 0). \end{aligned}$$

Donc R et P ont même partir lacunaire d'après le lemme.

Donc $P = R + e_n P_1$, avec $f_1 \in A[X_1, \cdots, X_n]^{\mathfrak{S}_n}$. On a $d^\circ P_1 = d - n < d$. Donc par hypothèse de récurrence sur d, il existe $Q_1 \in A[Y_1, \cdots, Y_n]$ tel que $P_1 = Q_1(e_1, \cdots, e_n)$. Donc $P \in A[e_1, \cdots, e_n]$. Cela prouve l'existence : $Q = \widetilde{Q} + e_n Q_1$.

Montrons l'unicité. S'il existe $Q', Q'' \in A[Y_1, \cdots, Y_n]$ tels que $Q'(e_1, \cdots, e_n) = Q''(e_1, \cdots, e_n)$, on a $Q(e_1, \cdots, e_n) = 0$ avec $Q = Q' - Q''$. On montre que Q=0 par une double récurrence sur n et $d^\circ Q$.

Posons $Q = Q_0 + Y_1 \cdots Y_n Q_1$ avec Q_0 lacunaire. On a $\widetilde{Q_0}(e_1, \cdots, e_{n-1}, 0) = 0$. Donc $\widetilde{Q_0} = 0$ d'après la récurrence. Donc $Q_1 = 0$. Donc $Q = 0$ car $d^\circ Q_1 < d^\circ Q$. □

Théorème 1.3.6. *(formule de Newton) Pour k entier≥ 0, on pose $\pi_k = \sum_{i=1}^n X_i^k$. On a*

$$k e_k = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i} \pi_i \qquad \textit{pour } k \leq n$$

et

$$0 = \sum_{i=k-n}^{k} (-1)^{i-1} e_{k-i} \pi_i \qquad \textit{pour } k > n.$$

En particulier, on trouve

$$\begin{aligned} &e_1 = \pi_1,\ 2e_2 = \pi_1^2 - \pi_2,\ 3e_3 = \frac{1}{2}\pi_1^3 - \frac{3}{2}\pi_1\pi_2 + \pi_3 \\ &4e_4 = \frac{1}{6}\pi_1^4 - \pi_1^2\pi_2 + \frac{4}{3}\pi_1\pi_3 + \frac{1}{2}\pi_2^2 - \pi_4,\ \cdots \end{aligned}$$

et

$$\pi_1 = e_1,\ \pi_2 = e_1^2 - 2e_2,\ \pi_3 = e_1^3 - 2e_1e_2 + 3e_3,\ \pi_4 = e_1^4 - 4e_1^2e_2 + 4e_1e_3.$$

Démonstration. Pour $n = k$, on pose

$$\prod_{i=1}^{k}(t - X_i) = \sum_{i=0}^{k}(-1)^{k-i}e_{k-i} \cdot t^i.$$

On spécialise en $t = X_j$. On trouve

$$0 = \sum_{i=0}^{k}(-1)^{k-i}e_{k-i}X_j^i.$$

Donc

$$\sum_{i=0}^{k}\sum_{j=1}^{n}(-1)^{k-i}e_{k-i}X_j^i = 0$$

et donc

$$\sum_{i=0}^{k}(-1)^{k-i}e_{k-i}\pi_i = 0.$$

Cela donne la formule pour $n = k$.
Pour les cas $n > k$ on peut obtenir par une récurrence. Le cas de n peut être réduit au cas de $n - 1$ en spécialisant $X_n = 0$, car les deux termes sont lacunaires et par le lemme précédent. Pour $k > n$, il suffit de remarquer que $e_k = 0$ si $k > n$(en fait, on pose $X_m = 0$ si $m > n$). □

1.4 Polynômes antissymétrique

Soit $P \in A[X_1, \cdots, X_n]$. On dit que P est alterné si pour tout $\tau \in \mathfrak{A}_n$ on a $\tau(P) = P$. On dit qu'il est antissymétrique si pour tout $\tau \in \mathfrak{S}_n$ on a $\tau(P) = \varepsilon(\tau)P$ où $\varepsilon(\tau)$ est la signature de τ. On pose $V_n = \prod_{1\leq i<j\leq n}(X_j - X_i)$. C'est le polynôme de Vandermonde. On a

$$V_n = \begin{vmatrix} 1 & X_1 & \cdots & X_1^{n-1} \\ 1 & X_2 & \cdots & X_2^{n-1} \\ \vdots & & & \vdots \\ 1 & X_n & \cdots & X_n^{n-1} \end{vmatrix}.$$

C'est un polynôme antissymétrique.

Remarques 1.4.1. *On a* $\prod_{1\leq i<j\leq n}(X_i - X_j) = (-1)^{\frac{n(n-1)}{2}}V_n$. *On pose* $\Delta_n = V_n^2$. *C'est le*

discriminant du polynôme $\prod_{i=1}^{n}(T-X_i)$. *On a* $\Delta_n \in A[X_1,\cdots,X_n]^{\mathfrak{S}_n}$. *Posons*

$$\Theta_n = \prod_{1\leq i<j\leq n}(X_i+X_j)$$
$$E_n = \frac{1}{4}(\Delta_n - \Theta_n^2)$$
$$W_n = \frac{1}{2}(V_n+\Theta_n).$$

On a $\Theta_n \in A[X_1,\cdots,X_n]^{\mathfrak{S}_n}$, $E_n \in A[X_1,\cdots,X_n]^{\mathfrak{S}_n}$, $W_n \in A[X_1,\cdots,X_n]^{\mathfrak{A}_n}$ *(polynôme alterné). On a* $\Theta_n \equiv V_n$ *modulo* 2 *car* $X_i+X_j = X_i - X_j$ *modulo* 2. *Donc*

$$\frac{V_n+\Theta_n}{2},\ \frac{V_n-\Theta_n}{2},\ E_n = \frac{V_n+\Theta_n}{2}\cdot\frac{V_n-\Theta_n}{2} \in \mathbb{Z}[X_1,\cdots,X_n].$$

Théorème 1.4.2. *Supposons* $n \geq 2$. *On a*

$$\underbrace{A[X_1,\cdots,X_n]^{\mathfrak{A}_n}}_{C} = \underbrace{A[X_1,\cdots,X_n]^{\mathfrak{S}_n}}_{B}[W_n].$$

Ou encore on a un isomorphisme de $A-$*algèbres*

$$\begin{array}{ccc} B[T]\Big/(T^2-\Theta_nT-E_n) & \xrightarrow{\sim} & C \\ Q & \longmapsto & Q(W_n). \end{array}$$

(on a $W_n^2-\Theta_nW_n-E_n=0$*)*
C'est aussi un isomorphisme de B-algèbre.

Corollaire 1.4.3. *Si* $n\geq 2$ *et* $2\in A^\times$ *tout polynôme antissymétrique est de la forme* V_nQ *avec* $Q\in A[X_1,\cdots,X_n]^{\mathfrak{S}_n}$.

Démonstration. (du corollaire) Soit P antissymétrique. Il est alterné. D'après le théorème, il s'écrit $P = R_0+R_1W_n$ avec $R_0,R_1\in A[X_1,\cdots,X_n]^{\mathfrak{S}_n}$. On a

$$P = R_0 + R_1\cdot\left(\frac{\Theta_n+V_n}{2}\right) = R_0+\frac{1}{2}\Theta_nR_1+\frac{1}{2}V_nR_1$$

car $2\in A^\times$. Soit $\tau\in\mathfrak{S}_n\backslash\mathfrak{A}_n$. On a

$$P-\tau(P) = (R_0+\frac{1}{2}\Theta_nR_1)-\tau(R_0+\frac{1}{2}\Theta_nR_1)+\frac{1}{2}V_nR_1-\frac{1}{2}\underbrace{\tau(V_n)}_{=-V_n}\underbrace{\tau(R_1)}_{=R_1} = V_nR_1.$$

□

Démonstration. (du théorème) On pose $B = A[X_1, \cdots, X_n]^{\mathfrak{S}_n}$, $C = A[X_1, \cdots, X_n]^{\mathfrak{A}_n}$. On va montrer que c'est un $B-$module libre de base $\{1, W_n\}$. Pour cela il suffit de montrer que $\{1, W_n\}$ engendre C comme $B-$module et que c'est une famille libre.

Soit $P \in C$. Soit $\tau \in \mathfrak{S}_n \backslash \mathfrak{A}_n$. Posons $P^- = P - \tau(P)$. Il est antissymétrique. Pour $\tau = (i\ j)$ (transposition), on a $\tau(P^-) = -P^-$ et donc $P^- = 0$ si on spécialise en $X_i = X_j$. Donc $X_i - X_j$ divise P^- pour tous $i, j \in \{1, \cdots, n\}$.

Remarques 1.4.4. *X_i n'est pas un diviseur de 0 dans $A[X_1, \cdots, X_n]$, et $X_i - X_j$ l'est ($i < j$), donc V_n l'est.*

Lemme 1.4.5. *Montrons que V_n divise P^-.*

Démonstration. Soit $F = \{(i, j) \in \{1, ..., n\} | i < j\}$. Soit $E \subset F$. Supposons que $\prod_{(i,j)\in E} (X_j - X_i)$ divise P^-. Soit $(u, v) \in F \setminus E$. Posons

$$P^- = \prod_{(i,j)\in E} (X_j - X_i) P_1 \qquad (*)$$

Montrons que $X_u - X_v$ divise P_1. Il divise P^-. Spécialisons $(*)$ en $X_u = X_v$. On trouve

$$0 = \prod_{(i,j)\in E} (X_i - X_j)_{X_u = X_v} P_1 \Big|_{X_u = X_v} \qquad (1.4.1)$$

Comme $(u, v) \notin E$, on a la première terme ne soit pas diviseur de 0. Donc on a que $P_1 \Big|_{X_u = X_v} = 0$. Donc $X_u - X_v$ divise P_1. Comme pour $E = \emptyset$, on a $\prod_{(i,j)\in E}$ divise P, par une récurrence on a V_n divise P. □

Revenons au théorème. Comme V_n n'est pas un diviseur de 0, P^- s'écrit de façon unique

$$P^- = V_n Q, Q \in A[X_1, \cdots, X_n]^{\mathfrak{S}_n} \qquad (1.4.2)$$

Posons $P^+ = P - W_n Q$. Montrons que P^+ est symétrique. Soit $\sigma \in \mathfrak{S}_n \setminus \mathfrak{A}_n$ et montrons que $\sigma(P^+) = P^+$. On a

$$\sigma(W_n) = \sigma\left(\frac{1}{2}(\Theta_n + V_n)\right) = \frac{1}{2}(\Theta_n - V_n)$$

Donc

$$\begin{aligned}\sigma(P^+) &= \sigma(P) - \sigma(W_n)\sigma(Q)\\ &= \sigma(P) - \frac{1}{2}(\Theta_n - V_n)Q\\ &= P - P^- + V_nQ - W_nQ\\ &= P^+\end{aligned}$$

Donc $P = P^+ + W_nQ \in B + w_nB$. On a bien des générateurs de C. Montrons que $\{1, W_n\}$ est libre. Soit $Q_1, Q_2 \in B$ tels que $Q_1 + Q_2W_n = 0$. On a pour $\sigma \in \mathfrak{S}_n \setminus \mathfrak{A}_n$

$$-\sigma(Q_1) = -Q_1 = \sigma(Q_2)\sigma(W_n) = Q_2(w_n - V_n)$$

car $-Q_1 = Q_2W_n$. Donc $W_nQ_2 = (W_n - V_n)Q_2$, et puis $Q_2 = 0$, et $Q_1 = 0$. Donc la famille $\{1, W_n\}$ est libre. □

1.5 Le lemme de normalisation de Noether

Théorème 1.5.1. *(lemme de normalisation de Noether) Soit K un corps. Soit A une $K-$algèbre commutative de type fini. Il existe un entier $d \geq 0$ et $y_1, \cdots, y_d \in A$ algébriquement indépendants sur K tels que A est un module de type fini sur $K[y_1, \cdots, y_d]$.*

Démonstration. Il existe $u_1, \cdots, u_m \in A$ tels que $A = K[u_1, \cdots, u_m]$. On procède par récurrence sur m. Si $m = 0$, OK. On suppose que le théorème est vrai pour les $K-$algèbres engendrée par $m-1$ éléments. Il suffit de montrer qu'il existe $B \subset A$ une sous-K-algèbre, avec $A = B-$module de type fini, et B engendré par $m-1$ éléments comme $K-$algèbre.

Si $u_1, \cdots, u_m$ sont algébriquement indépendants, c'est terminé. Donc on suppose qu'il existe $P \in K[X_1, \cdots, X_m]$, $P \neq 0$ avec $P(u_1, \cdots, u_m) = 0$.

Posons

$$P(X_1, \cdots, X_m) = \sum_{\alpha_1, \cdots, \alpha_m} a_{\alpha_1, \cdots, \alpha_m} X_1^{\alpha_1} \cdots X_m^{\alpha_m}$$

avec $a_{\alpha_1, \cdots, \alpha_m} \in K$. Posons r entier$> \{\alpha_1, \cdots, \alpha_m \mid a_{\alpha_1, \cdots, \alpha_m} \neq 0\}$.

Remarque fondamentale : Si $a_{\alpha_1,\cdots,\alpha_m} \neq 0$ et $a_{\beta_1,\cdots,\beta_m} \neq 0$, on a

$$\alpha_1 + \alpha_2 r + \cdots + \alpha_m r^{m-1} \neq \beta_1 + \beta_2 r + \cdots + \beta_m r^{m-1}$$

si $(\alpha_1, \cdots, \alpha_m) \neq (\beta_1, \cdots, \beta_m)$. Posons $z_i = u_i - z_1^{r^{i-1}}$ pour $2 \leq i \leq m$. Alors

$$\begin{aligned} 0 &= P(u_1, z_2 + u_1^r, \cdots, z_m + u_1^{r^{m-1}}) \\ &= \sum_{\alpha_1,\cdots,\alpha_m} a_{\alpha_1,\cdots,\alpha_m} \underbrace{u_1^{\alpha_1}(z_2 + u_1^r)^{\alpha_2} \cdots (z_m + u_1^{r^{m-1}})}_{\substack{u_1^{\alpha_1+\alpha_2 r+\cdots+\alpha_m r^{m-1}} + termes \\ de\ plus\ petits\ degré\ en\ u_1}}. \end{aligned}$$

Quand $(\alpha_1, \cdots, \alpha_m)$ varient ces degrés sont tous différents.

Donc ce polynôme$\in K[z_2, \cdots, z_m][u_1]$. Le coefficient dominant est dans K. Donc u_1 est entier sur $K[z_2, \cdots, z_m]$. Posons $B = K[z_2, \cdots, z_m]$. Donc $u_i = z_i + u_1^{r^{i-1}}$ est entier sur B. Comme $A = K[z_1, \cdots, z_m]$, A est entier sur B. Donc A est de type fini sur B. Comme B est une algèbre engendrée par $z_2, \cdots, z_m$, on a terminé. □

Remarques 1.5.2. *1. L'entier d est bien défini. C'est la dimension de Krull de A.*

2. Si A est intègre, d est le degré de transcendance de Frac(A) *sur K.*

1.6 Le radical d'un idéal

Soit A un anneau. Soit $a \in A$. Il est dit nilpotent s'il existe un entier $n \geq 1$ tel que $a^n = 0$. On pose $\sqrt{0} = \{a \in A \mid a\ nilpotent\}$. C'est le nilradical de A.

Proposition 1.6.1. *C'est un idéal de A.*

Démonstration. On a $0 \in \sqrt{0}$. Soient $a, b \in \sqrt{0}$. On a $a^n = 0$ et $b^m = 0$. Donc $(a+b)^k = \sum_{i=0}^{k} C_k^i a^i b^{k-i} = 0$ si $k > m+n$. Donc $a + b \in \sqrt{0}$. Pour $c \in A$, on a $(ac)^n = a^n c^n = 0$. Donc $ac \in \sqrt{0}$. □

Pour l'idéal de A, on pose $\sqrt{I} = \{a \in A \mid il\ existe\ n \geq 1\ avec\ a^n \in I\}$. C'est le radical ou la racine de I. C'est l'image inverse de $\sqrt{0}$ par $A \to A/I$ (morphisme d'anneau). Donc, comme l'image inverse d'un idéal est un idéal, $\sqrt{I}$ est un idéal de A.

Proposition 1.6.2. *Si $\sqrt{I}$ est de type fini sur A, il existe n entier≥ 1 tel que $(\sqrt{I})^n \subset I$.*

Démonstration. Soit $(x_1, \cdots, x_k)$ un système de générateurs de $\sqrt{I}$. Soit $a_1, \cdots, a_n \in A$. Pour tout $1 \leq i \leq n$, il existe $\lambda_1^{(i)}, \cdots, \lambda_k^{(i)} \in A$ tels que $x = \lambda_1^{(i)} x_1 + \cdots + \lambda_k^{(i)} x_k$. On a

$$a_1 \cdots a_n = (\lambda_1 x_1 + \cdots + \lambda_k x_k)^n = \sum_{e_1 + \cdots + e_k = n} \star x_1^{e_1} \cdots x_k^{e_k}$$

Comme $u > \sum_{i=1}^{k} n_i$, il existe i tel que $e_i > i$. Donc $x_i^{n_i} \in I$. Donc $x^n \in I$. □

Proposition 1.6.3. *Supposons A noethérien. Soient I et J des idéaux de A. On a $\sqrt{I} = \sqrt{J}$ si et seulement s'il existe k, l entiers≥ 1 avec $I^k \subset J$ et $J^l \subset I$.*

Démonstration. Application directe de la proposition précédent. □

Proposition 1.6.4. *On a $\sqrt{\sqrt{I}} = \sqrt{I}$.*

Démonstration. Soit $x \in \sqrt{\sqrt{I}}$. Il existe $n \geq 1$ tel que $x^n \in \sqrt{I}$. Il existe $m \geq 1$ tel que $(x^n)^m \in I$. Donc $x \in \sqrt{I}$. □

Proposition 1.6.5. *Si I est un idéal premier, on a $\sqrt{I} = I$.*

Démonstration. Soit $x \in \sqrt{I}$. Il existe $n \geq 1$ tel que $x^n \in I$. Comme I est premier, on a $x \in I$. □

Proposition 1.6.6. *On a $\sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J}$.*

Proposition 1.6.7. *On a $\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \supset I \\ \text{idéal} \\ \text{permier}}} \mathfrak{p}$.*

Démonstration. " $\subset$ " : Soit $\mathfrak{p}$ un idéal premier avec $I \subset \mathfrak{p}$. On a $\sqrt{I} \subset \sqrt{\mathfrak{p}} = \mathfrak{p}$.
" $\supset$ " : Réciproquement, soit $x \in A \backslash \sqrt{I}$. Soit

$$S = \{\text{idéaux } J \text{ tels que } I \subset J \text{ et tels que } x^{\mathbb{N}} \cap J = \varnothing\}$$

où

$$x^{\mathbb{N}} = \{1, x, x^2, \cdots\}.$$

On a $S \neq \varnothing$ car $1 \in S$. Par le lemme de Zorn il existe J_0 maximal pour l'inclusion dans S. Montrons que J_0 est un idéal premier. Soient $b, b' \in A$ tels que $bb' \in J_0$, avec $b \in J_0, b' \in J_0$.

Comme J_0 est maximal pour l'inclusion, on a $(J_0 + Ab) \cap x^{\mathbb{N}} \neq \varnothing$ et $(J_0 + Ab') \cap x^{\mathbb{N}} \neq \varnothing$. Il existe $c, c' \in J_0$, $a, a' \in A$, n, n' entiers≥ 1 tels que $x^n = c + ab$ et $x^n = c' + a'b'$. Donc $x^{n+m'} = \underbrace{cc'}_{\in J_0} + \underbrace{abc'}_{\in J_0} + \underbrace{a'b'c}_{\in J_0} + \underbrace{aba'b'}_{\in J_0} \in J_0$. Absurde car $J_0 \cap x^{\mathbb{N}} = \varnothing$. □

1.7 Le théorème des zéros (Nullstellensatz de Hilbert)

Théorème 1.7.1. *(lemme de Zariski) Soit L un corps. Soit K un sous-corps de L tel que L est une K-algèbre de type fini. Alors L est une extension algébrique de K (et donc une extension finie de K)*

Démonstration. Posons $L = K(z_1, \cdots, z_d)$ avec $z_1, \cdots, z_d \in L$ et d minimal. Récurrence sur d. Si $z_1, \cdots, z_d$ sont algébriques sur K, OK. Sinon, disons que z_1 n'est pas algébrique sur K. Alors $K(z_1) = Frac(K[z])$ est un sous-corps de L. Par récurrence on a que $z_2, \cdots, z_d$ sont algébrique sur $K(z_1)$. Il existe $P_2, \cdots, P_d \in K[z_1]$ tel que $P_2 z_2, \cdots, P_d z_d$ sont entier sur $K[z_1]$. Donc, en posant $P = P_2 \cdots P_d, Pz_2, \cdots, Pz_d$ sont entiers sur $K[z_1]$. Soit $f \in L$. Pour N assez grand, on a $P^N f \in K[z_1, Pz_2, \cdots, Pz_d]$. Donc $P^N f$ est entier sur $K[z_1]$. Car $K[z_1]$ est intégralement clos, on a que

$$K(z_1) = \bigcup_{N>0} \frac{1}{P^N} K[z_1]$$

Absurde car il existe $F = \frac{R}{Q}$ avec Q premier à P et R premier à Q. □

Notation : $\bar{K}$ désigne une clôture algébrique d'un corps.
Si$a_1, \cdots, a_k \in A$, où A est un anneau, on pose $(a_1, \cdots, a_k) = idalengendrpara_1, \cdots, a_k = Aa_1 + \cdots + Aa_k$

Théorème 1.7.2. *(Nullstellensatz faible) Soit K un corps. Soit n un entier ≥ 1. Soit I$\subset$ $K[X_1, \cdots, X_n]$ un idéal avec $I \neq K[X_1, \cdots, X_n]$. Il existe $a_1, \cdots, a_n \in \bar{K}^n$ tels que pour tout $f \in I$, on a $f(a_1, \cdots, a_n) = 0$.*

Démonstration. Soit m un idéal maximal de $K[X_1, \cdots, X_n]$ avec $I \subset m$. Il existe par le lemme de Zorn et $I \neq K[X_1, \cdots, X_n]$. Alors $K[X_1, \cdots, X_n]/m$ est un corps et une algèbre de type fini sur K. Par le lemme de Zariski, c'est une extension finie de K. Elle se prolonge dans $\bar{K}$. On a donc un morphisme d'anneau

$$K[X_1, \cdots, X_n] \longrightarrow K[X_1, \cdots, X_n]/I \longrightarrow K[X_1, \cdots, X_n]/m \longrightarrow \bar{K}$$

Soient $a_1, \cdots, a_n \in \bar{K}$ les images de $X_1, \cdots, X_n$. On a bien $f(a_1, \cdots, a_n) = 0$ pour $f \in I$. □

Corollaire 1.7.3. *Supposons le corps K algébriquement clos, i.e. $K = \bar{K}$. Les idéaux maximaux de $K[X_1, \cdots, X_n]$ sont de la forme $(X_1 - a_1, \cdots, X_n - a_n)$ avec $a_1, \cdots, a_n \in K$.*

Démonstration. Soit $(a_1, \cdots, a_n) \in K^n$. On a un morphisme surjectif

$$K[X_1, \cdots, X_n] \longrightarrow K$$

(évaluation en $(a_1, \cdots, a_n)$). Son noyau est un idéal maximal car K est un corps. c'est $(X_1 - a_1, \cdots, X_n - a_n)$. Réciproquement, soit m un idéal maximal de K$[X_1, \cdots, X_n]$. Par le théoème des zéros faible, il existe $(a_1, \cdots, a_n) \in \bar{K}^n$ tel que pour tout $f \in m$ on a $f(a_1, \cdots, a_n) = 0$. Écrivon f comme un polynôme en $(X_1 - a_1), \cdots, (X_n - a_n)$. Le terme constante est $f(a_1, \cdots, a_n)$. Donc $f \in (X_1 - a_1, \cdots, X_n - a_n)$. Donc $m = (X_1 - a_1, \cdots, X_n - a_n)$ □

Pour I idéal de $K[X_1, \cdots, X_n]$, on pose

$$V(I) = \{(a_1, \cdots, a_n) \in K^n \mid \forall f \in I, f(a_1, \cdots, a_n) = 0\}$$

C'est le lieu d'annulation de I.

Théorème 1.7.4. *(Nullstellensatz fort)*
Soit I un idéal de $K[X_1, \cdots, X_n]$. Soit $h \in K[X_1, \cdots, X_n]$ tel que $h(V(I)) = \{0\}$. Il existe un entier $n \geq 1$ tel que $h^n \in I$. (ou encore, on a $h \in \sqrt{I}$).

Démonstration. On suppose que $h \neq 0$. Comme $K[X_1, \cdots, X_n]$ est nothérien, I est de type fini. Il existe $g_1, \cdots, g_m \in K[X_1, \cdots, X_n]$ tels que $I = (g_1, \cdots, g_m)$. Alors

$$V(I) = \{(a_1, \cdots, a_n) \in \bar{K}^n, g_1(a_1, \cdots, a_n) = \cdots = g_m(a_1, \cdots, a_n) = 0\}$$

Posons

$$W_h(I) = \left\{ (a_1, \cdots, a_n, b) \in \bar{K}^{n+1} \;\middle|\; \begin{array}{c} g_1(a_1, \cdots, a_n) = \cdots = g_n(a_1, \cdots, a_n) = 0 \\ et\ 1 - bh(a_1, \cdots, a_n) = 0 \end{array} \right\}$$

C'est le lieu d'annulation de $(g_1, \cdots, g_m, 1 - yh)$ dans $K[X_1, \cdots, X_n, Y]$. Si $(a_1, \cdots, a_n) \in V(I)$, on a $h(a_1, \cdots, a_n) = 0$ on a $1 - bh(a_1, \cdots, a_n) \neq 0$. Donc $W_h(I) = \varnothing$. D'après le théorème des zéros faible on a $(g_1, \cdots, g_m, 1 - yh) = K[X_1, \cdots, X_n, Y]$. Donc $1 \in (g_1, \cdots, g_m, 1 -$

yh). Donc il existe $f_1, \cdots, f_m, f_{m+1} \in K[X_1, \cdots, X_n, Y]$ avec $1 = \sum_{i=1}^{m} f_i g_i + f_{m+1}(1 - yh)$. Considérons

$$\begin{aligned} K[X_1, \cdots, X_n, y] &\longrightarrow K(X_1, \cdots, X_n) = Frac(K[X_1, \cdots, X_n]) \\ y &\longmapsto h^{-1} \end{aligned}$$

(spécialisation de y en $h^{-1} \in K(X_1, \cdots, X_n)$). Revenons à

$$1 = \sum_{i=1}^{m} f_i g_i + f_{m+1}(1 - yh)$$

On spécialise en $y = h^{-1}$. On trouve

$$1 = \sum_{i=1}^{m} f_i(X_1, \cdots, X_n, h^{-1}) g_i(X_1, \cdots, X_n)$$

Or $f_i(X_1, \cdots, X_n, h^{-1}) = \frac{P_i(X_1, \cdots, X_n)}{h^{k_i}}$, avec $P_i(X_1, \cdots, X_n) \in K[X_1, \cdots, X_n]$ et k_i entier ≥ 0. Posons $k = \max\{k_i | 1 \leq i \geq m\}$. On a donc

$$1 = \sum_{i=1}^{m} \frac{P_i(X_1, \cdots, X_n)}{h^{k_i}} g_i$$

et donc

$$h^k = \sum_{i=1}^{m} \underbrace{h^{k-k^i}}_{\in K[X_1, \cdots, X_n]} \underbrace{P_i(X_1, \cdots, X_n)}_{\in K[X_1, \cdots, X_n]} \underbrace{g_i}_{\in I}$$

Donc $h^k \in I$ et donc $h \in \sqrt{I}$. □

Chapitre 2

Le dictionnaire entre l'algèbre et la géométrie

2.1 Ensemble algébrique affine

Soit K un corps. Soit n un entier≥ 1. Soit $S \subset K[X_1, \cdots, X_n]$. Posons

$$V(S) = \{x \in K^n \mid \textit{pour tout } P \in S,\ P(x) = 0\}.$$

C'est l'ensemble algébrique affine défini sur S. On a $V(1) = \varnothing$, $V(0) = K^n$. Si $n = 1$, $V(S) = K$ ou $V(S)$ est fini. Si $S \subset T$, on a $V(T) \subset V(S)$ (l'application $S \mapsto V(S)$ est décroissante). On a $V(S) = V(\textit{idéal engendré par } S)$. Comme l'anneau $K[X_1, \cdots, X_n]$ est noethérien, tout idéal de cet anneau est de type fini. Donc il existe $P_1, \cdots, P_k \in K[X_1, \cdots, X_k]$ avec $V(S) = V(\{P_1, \cdots, P_k\})$, ou encore $V(S) = V(P_1) \cap \cdots \cap V(P_k)$. (on écrit $V(P_1, \cdots, P_k) = V(\{f_1, \cdots, f_k\})$)

Pour $P \in K[X_1, \cdots, X_n]$, on dit que $V(P)$ est une hypersurface. On a

$$\begin{aligned} V(X) &= \{x \in K | x = 0\} \\ &= \{x \in K | x^2 = 0\} \\ &= V(x^2) \end{aligned}$$

Donc $S \mapsto V(S)$ n'est pas injective. Si $a = (a_1, \cdots, a_n)$, on a $\{a\} = V(X_1 - a_1, \cdots, X_n - a_n)$. Tout singleton est un espace algébrique affine. Soit $(S_j)_{j \in J}$ une famille avec $S_j \in$

$V[X_1, \cdots, X_n]$, on a

$$\bigcap_{j\in J} V(S_j) = V\Big(\bigcup_{j\in J} S_j\Big) = V\Big(\sum_{j\in J} I_j\Big)$$

On a de plus $V(I) \cup V(J) = V(I \cap J)$. Donc tout ensemble fini$\subset K^n$ est un ensemble algébrique affine.

2.2 La topologie de Zariski

Soit X un ensemble. Soit Ω un ensemble de parties de X. On dit que Ω est une topologie sur X, si on a les propriétés suivantes :
$-$ $\varnothing \in \Omega,\ X \in \Omega$;
$-$ pour toute famille $(U_i)_{i\in I}$ d'éléments de Ω, on a $\bigcup_{i\in I} U_i \in \Omega$;
$-$ pour toute famille finie $(U_i)_{i\in I}$ d'élément de Ω, on a $\bigcap_{i\in I} U_i \in \Omega$.

On dit alors que (X, Ω) est un espace topologique. Les éléments de Ω s'appellent des ouverts. Les complémentaires des ouverts s'appellent des fermes. $\varnothing$, X sont fermés, une intersection des fermés est un fermé. Une réunion finie de fermés est un fermé.

Soit $Y \subset X$. $\Omega' = \{Y \cap U \mid U \in \Omega\}$ définit une topologie sur Y. On dit que (Y, Ω') est un sous-espace topologique de X et que Ω' est la topologie induite par Ω.

Soit $B \subset \Omega$. On dit que B est une base de la topologie Ω si tout ouvert est réunion d'éléments de B.

Exemples 2.2.1. espace métrique.

Soit X et Y deux espace topologiques. Soit $f : X \to Y$. On dit que f est continue si l'image réciproque d'un ouvert Y est un ouvert de X.

Revenons aux ensembles algébriques affines$\subset K^n$. Les complémentaires des ensembles algébriques affines sont les ouverts d'une topologie de K^n. C'est la topologie de Zariski.

Remarques 2.2.2. *topologie très étrange. Les ouverts sont très "gros".*

Pour $P \in K[X_1, \cdots, X_n]$, on dit que $K^n \backslash V(P)$ est un ouvert standard pour la topologie de Zariski.

Proposition 2.2.3. *Tout ouvert de K^n est réunion finie d'ouverts standards. En particulier, les ouverts standards forment une base de Zariski.*

Démonstration. Voir ci-dessus : $V(S) = \bigcap_{i=1}^{k} V(P_i)$ car $K[X_1, \cdots, X_n]$ est noethérien. □

2.3 L'idéal d'un ensemble algébrique affine

Soit $V \subset K^n$. Posons

$$I(V) = \{P \in K[X_1, \cdots, X_n] \mid \textit{Pour tout } v \in V, \textit{ on a } P(v) = 0\}.$$

C'est l'idéal associé à V.

Posons

$$\Gamma(V) = K[X_1, \cdots, X_n]/I(V)\ .$$

On a si $V \subset W$, $I(W) \subset I(V)$ ($V \mapsto I(V)$ est décrossante). On a $V(I(V)) = V$ (car $V \subset V(I(V))$ et si $V = V(I)$ on a $I \subset I(V)$ et donc $V(I) \supset V(I(V))$). L'application $V \to I(V)$ est injective. On a $I \subset I(V(I))$, mais pas $I = I(V(I))$ en général.

Exemples 2.3.1. $K = \mathbb{R}$, $n = 2$, $I = (X^2 + Y^2 + 1)$. On a $V(I) = \varnothing$ et $I(V(I)) = \mathbb{R}[X, Y]$.

Si K est algébriquement clos, on a $I(V(I)) = \sqrt{I}$ (Nullstellensatz). Si K est infini, on a $I(K^n) = 0$.

En effet, si $P \in I(K^n)$, on a $P(a_1, \cdots, a_n) = 0$ pour tout $(a_1, \cdots, a_n) \in K^n$. Si on fixe $a_1, \cdots, a_n$, $P(X, a_2, \cdots, a_n) = 0$. Donc par itération $P = 0$. Si K est un corps fini, à q éléments, on a $X_1^q - X_1 \in I(K^n)$, donc $I(K^n) \neq 0$.

2.4 Irréductibilité

Soit X un espace topologique. $X \neq \varnothing$.

Proposition 2.4.1. *Les assertions suivantes sont équivalentes :*

1. *Si $X = F \cup G$, avec F, G fermés, on a $X = F$ ou $X = G$;*

2. *Si $U, V \subset X$ sont ouverts, avec $U \cap V = \varnothing$, on a $U = \varnothing$ ou $V = \varnothing$;*
3. *Tout ouvert$\neq \varnothing$ de X est partout dense dans X.*

Lorsque ces propriétés sont vérifiés, on dit que X est irréductible.

Théorème 2.4.2. *Soit V un ensemble algébrique affine. Les conditions suivantes sont équivalentes :*

1. *V irréductible ;*
2. *$I(V)$ est un idéal premier ;*
3. *$\Gamma(V) = \Gamma(V) = K[X_1, \cdots, X_n]/I(V)$ est un anneau intègre.*

Démonstration. 2. $\Leftrightarrow$ 3. OK. Montrons 1. $\Leftrightarrow$ 2..
Supposons V irréductible. Soient $P, Q \in I(V)$. On a $V = V(I(V)) \subset V(I) \cup V(Q)$ et donc $V = (V(P) \cap V) \cup (V(Q) \cap V)$. Comme V est irréductible, on a $V = V(I) \cap V$ ou $V = V(Q) \cap V$. Donc $P \in I(V)$ ou $Q \in I(V)$. Donc $\Gamma(V)$ est un idéal premier.

Montrons 2. $\Leftrightarrow$ 1.. Supposons $I(V)$ premier et $V = V_1 \cup V_2$ avec V_1, V_2 fermés, $V_1 \neq V$, $V_2 \neq V$. On a $I(V) \subsetneqq I(V_1)$ et $I(V) \subsetneqq I(V_2)$. Il existe $P_1 \in I(V_1) - I(V)$, $P_1 \in I(V_2) - I(V)$ avec $P_1, P_2 = 0$ sur V. Donc $P_1, P_2 \in I(V)$. Absurde car $I(V)$ premier. □

Corollaire 2.4.3. *Supposons K infini. Alors. K^n est irréductible.*

Démonstration. On a vu que $I(K^n) = 0$ et $K[X_1, \cdots, X_n]$ est intègre. Donc $I(K^n)$ est premier. □

Théorème 2.4.4. *Soit V un ensemble algébrique affine non vide. On peut écrire de façon unique $V = V_1 \cup \cdots \cup V_r$ avec $V_1, \cdots V_r$ ensembles algébriques affines irréductibles avec $V_i \not\subset V_j$ pour $i \neq j$. Les $(V_i)_{1 \leq i \leq r}$ s'appellent les composantes irréductibles de V.*

Démonstration. Voyons l'existence. Soit E l'ensemble des ensembles algébriques affines qui ne s'écrivant pas comme réunion d'irréductibles. Soit $I(E)$ l'ensemble des idéals associes. Soit $V \in E$ tel que $I(V)$ soit maximal dans $I(E)$. Alors V n'est pas irréductible. On a $V = F \cup G$ où F et G sont fermés. On a $F \neq V$, $G \neq V$. Donc $I(F) \supsetneqq I(V)$ et $I(G) \supsetneqq I(V)$. Comme $I(V)$ est maximal dans $I(E)$, on a $I(F)$ et $I(G)$ décomposables. Posons $F = F_1 \cup \cdots \cup F_r$, $G = G_1 \cup \cdots \cup G_s$ avec $F_1, \cdots, F_r, G_1, \cdots, G_s$ irréductibles. Donc $V = F_1 \cup \cdots \cup F_r \cup G_1 \cup \cdots \cup G_s$. Absurde. Donc V est décomposable en réunion d'irréductibles.

Montrons l'unicité de la décomposation. Supposons que $V = V_1 \cup \cdots \cup V_r = W_1 \cup \cdots \cup W_s$. On écrit $V_i = V \cap V_i = (W_1 \cap V_i) \cup \cdots \cup (W_s \cap V_i)$. Il existe j tel que $W_j \cap V_i = V_i$ car V_i est irréductible. Donc $V_i \subset W_j$. Par un raisonnement analogue, il existe k tel que $W_j \subset V_k$. Donc $V_j \subset V_k$. Donc $i = k$ et alors $V_i = W_j$. On a de plus r=s. D'où l'unicité. □

Les composantes irréductibles sont les sous-ensembles fermés irréductibles maximaux de V.

2.5 Application de Nullstellensatz

Soit I un idéal d'un anneau A. On dit que c'est un idéal radical si on a $I = \sqrt{I}$. C'est le cas des idéaux premiers.

Proposition 2.5.1. *L'application $W \mapsto I(W)$ est une bijection entre les ensembles algébriques affines de K^n et les idéaux radicaux de $K[X_1, \cdots, X_n]$.*

De plus W est irréductible ssi $I(W)$ est premier ssi $\Gamma(W)$ est intègre. De plus W est un singleton ssi I(W) est maximal ssi $\Gamma(W)$ est un corps.

Démonstration. Résulte du Nullstellensatz. □

Proposition 2.5.2. *Soit $V \subset K^n$ un ensemble algébrique affine. On a V fini ssi $\Gamma(V)$ est un $K-$espace vectoriel de dimention finie.*

Démonstration. Supposons V fini. Posons $V = \{u_1, \cdots, u_r\}$. On a un morphisme de $K-$espaces vectoriels

$$\begin{aligned} \varphi : K[X_1, \cdots, X_n] &\longrightarrow K^r \\ P &\longmapsto (P(u_1), \cdots, P(u_r)). \end{aligned}$$

Cela permet de plonger $\Gamma(V) = K[X_1, \cdots, X_n]/I(V)$ dans K^r. Donc $\Gamma(V)$ est un $K-$espace vectoriel de dimension finie.

Réciproquement, supposons $\Gamma(V)$ de dimension finie sur K. Notons $\overline{X_i}$ la classe de X_i dans $\Gamma(V)$. La famille $(\overline{X_i}^k)_{k\geq 0}$ est liée car $\Gamma(V)$ de dimension finie. Il existe $a_0, a_1, \cdots, a_s \in K$ tels que $a_0 + a_1\overline{X_1} + \cdots + a_s\overline{X_1}^s = 0$, avec $a_s \neq 0$. Donc, pour $(x_1, \cdots, x_n) \in V$, on a

$a_0 + a_1 x_1 + \cdots + a_s x_1^s = 0$.

Donc x_1 est racine de $P_1 \in K[X]$.

De même x_2 est racine de $P_2 \in K[X]$.

...

De même x_n est racine de $P_n \in K[X]$.

Donc $(x_1, \cdots, x_n) \in \underbrace{P_1^{-1}(0)}_{fini} \cap \cdots \cap \underbrace{P_n^{-1}(0)}_{fini}$, et donc V est fini. □

Soit $W \subset V$ deux ensembles algébriques affines. Alors $I(V) \subset I(W)$. Donc notons $I_V(W)$ l'image réciproque de $I(W)$ dans $\Gamma(V)$. On a $\Gamma(V)/I_V(W) \simeq \Gamma(W)$. On a $I_V(W)$ radical.

Proposition 2.5.3. *Les applications $W \mapsto I_V(W)$ et $I \mapsto V(I)$ sont des bijections décroissantes et réciproques entre les ensembles algébriques affines contenues dans V et les idéaux radicaux de $\Gamma(V)$.*

1. *De plus, on a W irréductible ssi $I_V(W)$ est premier ssi $\Gamma(W)$ est intègre.*
2. *On a W est un singleton ssi $I_V(W)$ est maximal ssi $\Gamma(V)$ est isomorphe à K.*
3. *On a W est une composante irréductible de V ssi $I_V(W)$ est un idéal premier maximal de $\Gamma(V)$.*

Démonstration. bijection claire.

1. OK.
2. Soit $x \in V$. Alors on a un morphisme de $K-$algèbres $\Gamma(V) \longrightarrow K$, $P \longmapsto P(x)$ surjectif de noyau l'idéal maximal $I(\{x\})$. D'où $\Gamma(W) = \Gamma(W)/I(\{x\}) \simeq K$.
3. résulte du fait que les composantes irréductibles, par définition, sont les fermés maximaux.

□

Les morphismes $\Gamma(W) \to K$ s'appellent les caractères de $\Gamma(W)$.

Proposition 2.5.4. *Les points de V sont en bijection avec les caractères de $\Gamma(V)$ (C'est à dire avec les idéaux maximaux de $\Gamma(V)$).*

2.6 Équivalence de catégories

Une catégorie $\mathscr{C}$, consiste en des objets regroupés dans $\mathscr{O}b(\mathscr{C})$, pour tous X, Y objets de $\mathscr{C}$, un ensemble de morphismes noté $Hom_{\mathscr{C}}(X, Y)$ avec une loi de composition $\circ$ pour X, Y, Z objets de $\mathscr{C}$ on a

$$\begin{aligned} Hom_{\mathscr{C}}(X,Y) \times Hom_{\mathscr{C}}(Y,Z) &\longrightarrow Hom_{\mathscr{C}}(X,Z) \\ (f,g) &\longrightarrow g \circ f. \end{aligned}$$

de telle sorte que : "$\circ$" est associative et pour tout X objet de $\mathscr{C}$, il existe $id_X \in Hom_{\mathscr{C}}(X, X)$ avec pour tout $f \in Hom_{\mathscr{C}}(X, Y)$, on a $f \circ id_X = f = id_Y \circ f$. Alors id_X est unique.

Soit $f \in Hom_{\mathscr{C}}(X, Y)$. X s'appelle la source de f. Y s'appelle le but de f.

On dit que f est un monomorphisme (resp. épimorphisme) si pour tout g_1, g_2 on a $f \circ g_1 = f \circ g_2$ (resp. $g_1 \circ f = g_2 \circ f$) entraîne $g_1 = g_2$.

On dit que $f \in Hom_{\mathscr{C}}(X, Y)$ est un isomorphisme s'il existe $g \in Hom_{\mathscr{C}}(Y, X)$ avec $g \circ f = id_X$ et $f \circ g = id_Y$.

On dit que $\mathscr{C}$ est finie si elle n'a que au nombre fini d'objet et que pour tous objets X et Y de $\mathscr{C}$, $Hom_{\mathscr{C}}(X, Y)$ est fini.

On dit que $\mathscr{C}$ est discrète si pour tous objets X, Y de $\mathscr{C}$, on a $Hom_{\mathscr{C}}(X, Y) \subset \{id_Y\}$.

On dit que $\mathscr{C}$ est un groupoïde si tout morphisme est un isomorphisme.

On dit que $\mathscr{C}$ est une petite catégorie si ses objets consistent un ensemble. Même si $\mathscr{O}b(\mathscr{C})$ n'est pas un ensemble, on écrira $X \in \mathscr{O}b(\mathscr{C})$ pour dire que X est un objet. de $\mathscr{C}$.

On appelle catégorie opposée à $\mathscr{C}$ et on note $\mathscr{C}^{op}$ la catégorie dont les objets sont $\mathscr{O}b(\mathscr{C})$ mais telle que $Hom_{\mathscr{C}}(X, Y) = Hom_{\mathscr{C}}(Y, X)$ (en renversant l'ordre pour la composition).

Soit $\mathscr{C}'$ une autre catégorie. On dit que c'est une sous-catégorie (resp. sous-catégorie pleine, resp. sous-catégorie saturée) si $\mathscr{O}b(\mathscr{C}') \subset Ob(\mathscr{C})$ et pour $X, Y \in \mathscr{O}b(\mathscr{C})$ on a $Hom_{\mathscr{C}'}(X,Y) \subset Hom_{\mathscr{C}}(X,Y)$ (resp. $Hom_{\mathscr{C}'}(X,Y) = Hom_{\mathscr{C}}(X,Y)$, resp. pour tout $X \in \mathscr{O}b(\mathscr{C}')$ tel que X et X' sont isomorphes). On dit que deux objets X, X' sont isomorphes dans $\mathscr{C}$ s'il existe un isomorphes dans $Hom_{\mathscr{C}}(X,X')$.

Exemples 2.6.1.

1. On note $\mathcal{E}ns$ la catégorie des ensemble dont les objets sont les ensembles et pour $E, F \in \mathscr{O}b(\mathscr{C})$ on a $Hom_{\mathcal{E}ns}(E,F) = \{application\ E \to F\}$.
2. On note $\mathcal{G}rp$ la catégorie des groupes dont les morphismes sont les morphismes de groupes.
3. De même on a la catégorie des groupes abéliens (sous-catégorie pleine de la catégorie des groupes).
4. La catégorie des ensembles finis est une sous-catégorie pleine de $\mathcal{E}ns$.
5. Si A est un anneau, on note $\mathcal{M}od(A)$ la catégorie des $A-$modules, dont les morphismes sont les morphismes de $A-$modules.
6. Si $A = K$ est un corps, c'est la catégorie des $K-$espaces vectoriels.
7. La catégorie de $A-$modules de type fini est une sous-catégorie pleine de la catégorie des $A-$module.
8. On note $\mathcal{T}op$ la catégorie des espaces topologiques dont les morphismes sont les applications continues.

Soient $.C$ et $\mathscr{C}'$ deux catégories. Un foncteur F de $\mathscr{C}$ vers $\mathscr{C}'$ associe à tout $X \in \mathscr{C}b(\mathscr{C})$, $F(X) \in \mathscr{C}'$ et tout $f \in Hom_{\mathscr{C}}(X,Y)$. $F(f) \in Hom_{\mathscr{C}'}(F(X), F(Y))$ avec les propriétés

$$F(id_X) = id_{F(X)}\ et\ F(f \circ g) = F(f) \circ F(g).$$

On dit encore que c'est un fonteur contravariant vérifie

$$F(f \circ g) = F(g) \circ F(f)\ au\ lieu\ de\ F(f \circ g) = F(f) \circ F(g).$$

On a un foncteur contravarient $op : \mathscr{C} \to \mathscr{C}^{op}$ avec $op(X) = X$ et $op(f) = f$.

Exemples 2.6.2. Notons $\mathcal{A}nn$ la catégories des anneaux. On a le foncteur $\mathcal{A}nn \to \mathcal{G}rp$ qui à A associe $A^{\times}$.

Soit $\mathcal{C}$ une catégorie. Soit $P \in \mathscr{O}b(\mathscr{C})$. On dit c'est un objet initial (resp. objet terminal) si pour tout $X \in \mathscr{O}b(\mathscr{C})$ on a $Hom_{\mathscr{C}}(P, X)$ (resp. $Hom_{\mathscr{C}}(X, P)$) est un singleton. Un objet initial et final est un zéro de la catégorie, souvent noté 0.

Exemples 2.6.3.
1. $\varnothing$ est un objet initial de $\mathcal{E}ns$, $\{a\}$ est un objet terminal de $\mathcal{E}ns$.
2. Le groupe trivial $\{1\}$ est un objet initial et terminal de $\mathcal{G}rp$.
3. L'anneau $\mathbb{Z}$ est un objet initial de $\mathcal{A}nn$, $\{0\}$ est un objet terminal de $\mathcal{A}nn$.
4. $\{0\}$ est un objet terminal et initial de $\mathcal{M}od(A)$.

Remarques 2.6.4. *tous les objtes initiaux (resp. terninaux) sont isomorphes.*

Soit F un foncteur d'une catégorie $\mathscr{C}$ vers une catégorie $\mathscr{C}'$, on dit. que F est fidèle (resp. plein, resp. pleinement fidèle) si l'application $Hom_{\mathscr{C}}(X, Y) \to Hom_{\mathscr{C}'}(F(X), F(Y))$ (qui à f associe $f(F)$) est injective (resp. surjective, resp. bijective). On dit que F est essentiellement surjectif si pour tout $X' \in \mathscr{O}b(\mathscr{C}')$, il existe $X \in \mathscr{O}b(\mathscr{C}')$ tel que X' est isomorphe à $F(X)$.

On dit que F est conservatif si pour tout $f \in Hom_{\mathscr{C}}(X, Y)$ tel que $F(f)$ est un isomorphisme on a que f est un isomorphisme.

Exercice 2.6.5.
1. $\mathcal{M}od(A) \to \mathcal{E}ns$ est fidèle et conservatif mais pas plein.
2. $\mathcal{T}op \to \mathcal{E}ns$ est fidèle mais ni plein ni conservatif.

Soient F_1 et F_2 deux fonctions de $\mathscr{C}$ vers $\mathscr{C}'$ un morphisme de foncteurs (ou transformation naturelle) de F_1 vers F_2 est notée $\theta : F_1 \to F_2$, tel que pour tout $X \in \mathscr{O}b(\mathscr{C})$ on a $\theta(X) \in Hom_{\mathscr{C}'}(F_1(x), F_2(X))$ tel que pour tout $f \in Hom_{\mathscr{C}}(X, Y)$ on a le diagramme

$$\begin{array}{ccc} F_1(X) & \xrightarrow{\theta(X)} & F_2(X) \\ {\scriptstyle F_1(f)}\downarrow & & \downarrow{\scriptstyle F_2(f)} \\ F_1(Y) & \xrightarrow{\theta(Y)} & F_2(Y) \end{array}$$

qui commute, i.e. $F_2(f) \circ \theta(X) = \theta(Y) \circ F_1(f)$. On schématise $\mathcal{C} \overset{F_1}{\underset{F_2}{\overset{\Downarrow\theta}{\rightrightarrows}}} \mathcal{C}'$.

On note $Fct(\mathscr{C}, \mathscr{C}')$ les foncteurs de $\mathscr{C}$ vers $\mathscr{C}'$. Ce sont les objets d'une catégorie (la catégorie des foncteurs de $\mathscr{C}$ vers $\mathscr{C}'$) dont les morphismes sont les morphismes de foncteurs.

Exemples 2.6.6. Pour K corps, on considère $\mathcal{M}od(K)^{op} \to \mathcal{M}od(K)$ qui à V associe $Hom_K(V,K) = V^*$ (dual de V). C'est un foncteur. Composé avec lui-même, cela donne un foncteur $\mathcal{M}od(K) \to \mathcal{M}od(K)$ qui à V associe $V^{**} = Hom_K(V^*,K)$ le bidual.

On a $\theta : id \to bidual$ un morphisme de foncteur defini par $\theta(V) = V^{**}$ (morphisme $V \to V^{**}$, $x \mapsto (\varphi \mapsto \varphi(x))$) car

$$\begin{array}{ccc} V & \xrightarrow{\theta(V)} & V^{**} \\ \downarrow & & \downarrow \\ W & \xrightarrow{\theta(W)} & W^{**} \end{array}$$

commute.

On dit qu'un foncteur $F : \mathscr{C} \to \mathscr{C}'$ est isomorphisme de catégories s'il existe un foncteur $G : \mathscr{C}' \to \mathscr{C}$ tel que $F \circ G = id_{\mathscr{C}'}$ et $G \circ F = id_{\mathscr{C}}$.

Pas une notion utile.

On dit que F est une équivalence de catégories s'il existe un foncteur $G : \mathscr{C}' \to \mathscr{C}$ tel que $F \circ G$ est isomorphe à $id_{\mathscr{C}'}$ et $G \circ F$ est isomorphe à $id_{\mathscr{C}}$. (isomorphe dans les catégories $Fct(\mathscr{C}', \mathscr{C}')$ et $Fct(\mathscr{C}, \mathscr{C})$)

Théorème 2.6.7. *Un foncteur est une équivalence de catégories ssi il est pleinement fidèle et eventiellement surject.*

Démonstration. Soit $F : \mathscr{C} \to \mathscr{C}'$. Suppose que F est une équivalence de catégories. Il existe un foncteur $G : \mathscr{C}' \to \mathscr{C}$ tel que $F \circ G \simeq id_Y$ et $G \circ F \simeq id_X$. Soit θ un morphisme de fonction $id_X \to G \circ F$. Pour tout $X, Y \in \mathscr{O}b(\mathscr{C})$ on a un diagramme commutatif

$$\begin{array}{ccccc} Hom_{\mathscr{C}}(X,Y) & \longrightarrow & Hom_{\mathscr{C}'}(F(X),F(Y)) & \longrightarrow & Hom_{\mathscr{C}}(G \circ F(X), G \circ F(Y)) \\ \downarrow{\scriptstyle id} & & & & \downarrow{\scriptstyle G \circ F(id)} \\ Hom_{\mathscr{C}}(X,Y) & & \longrightarrow & & Hom_{\mathscr{C}}(G \circ F(X), G \circ F(Y)) \end{array}$$

Notons θ^{-1} l'inverse de θ. En appliquant θ^{-1} on trouve que

$$Hom_{\mathscr{C}}(X,Y) \longrightarrow Hom_{\mathscr{C}'}(F(X),F(Y)) \longrightarrow Hom_{\mathscr{C}}(G \circ F(X), G \circ F(Y)) \longrightarrow Hom_{\mathscr{C}}(X,Y)$$

Donc F est pleinement fidèle.

Montrons que F est essentiellement surjectif. Pour tout $Y \in \mathscr{C}'$, on considère $G(Y)$ alors Y est isomorphe à $F \circ G(Y)$ par $\theta(Y) \in Hom(Y, F \circ G(Y))$.

Réciproquement si F est pleinement fidèle et essentiellement surjectif. Pour tout $Y \in \mathscr{O}b(\mathscr{C}')$ il existe $X \in \mathscr{O}b(\mathscr{C})$ et $\varphi_Y : Y \xrightarrow{\sim} F(X)$ isomorphisme. Soient $Y_1, Y_2 \in \mathscr{O}b(\mathscr{C}')$. On a

$$\begin{aligned} Hom_{\mathscr{C}'}(Y_1, Y_2) &= Hom_{\mathscr{C}'}(F(X_1), F(X_2)) \\ &\overset{pleine fidèlit}{=\!=\!=} Hom_{\mathscr{C}}(X_1, X_2). \end{aligned}$$

On pose $G(Y) = X$ et $G(f)$, pour $f \in Hom_{\mathscr{C}'}(Y_1, Y_2)$, est l'image de f dans $Hom_{\mathscr{C}}(X_1, X_2)$. On montre de G est un fonction. Montrons qu'on a un morphisme de foncteurs $\theta : id \to G \circ F$. On pose $\theta(X) \in Hom(X, G \circ F(X))$ ainsi on a $\varphi : F(X) \xrightarrow{\sim} F(G \circ F(X))$ par pleine fidèlité, il existe un isomorphisme $\theta(X) : X \to G \circ F(X)$. □

Exemples 2.6.8. Soit $\mathscr{C}$ la catégorie telle que $ob(\mathscr{C}) = \mathbb{N}$ et pour $n, m \in \mathbb{N}$ on pose $Hom_{\mathscr{C}}(n, m) = \underbrace{M_{n\times m}(K)}_{\substack{matrices \\ n\times m}}$ (K corp fixé). Soit $\mathcal{M}od(K)$ la catégorie de $K-$espaces vectoriels de dimension finie. On a le foncteur $F : \mathscr{C} \to \mathcal{M}od(K)$ tel que $F(n) = K^n$, et

$$F(M \in M_{n\times m}(K)) = endomorphisme\ K^n \to K^m\ de\ matrice\ M.$$

C'est une équivalence de catégorie.

Les morphismes sont plus importants que les objets !

2.7 Morphismes d'ensemble algébriques affines

Soient V, W des ensembles algébriques affines avec $V \subset K^n$, $W \subset K^m$, n, m entiers≥ 0. Soit $\varphi : V \to W$. Posons $\varphi = (varphi_1, \cdots, varphi_m)$ avec $\varphi_i : V \to K$. On dit que φ est régulière ou un morphisme d'éspece d'algébriques affines si pour tout i on a $\varphi_i \in \Gamma(V) = K[X_1, \cdots, X_n]/I(V)$. On pose $Reg(V, W) = \{application\ régulieres\ V \to W\}$. Cela donne une catégorie dont les objets sont les ensembles algébriques affines et les morphismes sont les

applications régulières. On a $\Gamma(V) \subset Reg(V, K)$.

Si $V = W = K^n$, les applications affines $K^n \to K^n$ sont régulières. Les projections $K^n \to K^m$, $m < n$, sont régulières.

Posons $V = V(Y - X^2) \subset K^2$ et $\varepsilon : V \to K$ donné par $\varphi(x, y) = x$. Alors φ est un isomorphisme de réciproque $x \mapsto (x, x^2)$. Considérons $\varphi : K \to V(X^3 + Y^3 - X^2) \subset K^2$ donnée par $\varphi(t) = (t^2 - 1, t(t^2 - 1))$ est un morphisme bijectif mais pas un isomorphisme.

Soit $\varphi : V \to W$ une application régulière. Poson $\varphi^* : \Gamma(W) \to \Gamma(V)$ qui à $f \in \Gamma(W)$ associe $\varphi^*(f) = f \circ \varphi$. Alors φ^* est un morphisme de $K-$algèbres $\Gamma(W) \to \Gamma(V)$. De plus, Γ est un foncteur de la catégorie des $K-$algèbres (contravariant car $(f \circ g)^* = g^* \circ f$).

Proposition 2.7.1. *Le foncteur Γ est pleinement fidèle.*
(l'application $Reg(V, W) \to Hom_{K-alg}(\Gamma(W), \Gamma(V))$ est bijective)

Soit Γ le foncteur contravarient de la catégorie des espaces algébriques affines vers la catégorie des $K-$algèbres. Il associe à V, l'algèbre $\Gamma(V) = K[X_1, \cdots, X_n]/I(V)$.

Proposition 2.7.2. *Ce foncteur est pleinement fidèle.*

Démonstration. Il faut montrer que pour tous V, W espaces algébriques affines et tout $\varphi : V \to W$ application régulière, $\varphi \mapsto \varphi^*$ est bijective.

Montrons qu'elle est injective. Soient φ, φ' tels que $\varphi^* = \varphi'^*$. On a $W \subset K^m$. Posons $\varphi = (\varphi_1, \cdots, \varphi_m)$ et $\varphi' = (\varphi'_1, \cdots, \varphi'_m)$. Notons $\overline{Y_i}$ l'image de Y_i dans $\Gamma(W)$. On a $\varphi^*(\overline{Y_i}) = \varphi'_i$ pour tout i, $1 \leq i \leq m$. Donc $\varphi = \varphi'$.

Montrons la surjectivité. Soit $\alpha : \Gamma(W) \to \Gamma(V)$ un morphisme de $K-$algèbre. On pose $\varphi_i = \alpha(\overline{Y_i})$ et $\varphi = (\varphi_1, \cdots, \varphi_m) : V \to K^m$: Montrons que $\varphi(V) \subset W$. Soit $F(Y_1, \cdots, Y_m) \in I(W)$. Soit $x \in V$. On a

$$\begin{aligned} F(\varphi(x)) &= F(\alpha(\overline{Y_1}), \cdots, \alpha(\overline{Y_m})(x) \\ &= \alpha(F(\overline{Y_1}, \cdots, \overline{Y_m}))(x) \end{aligned}$$

car α est un morphisme de $K-$algèbre. Or $F(\overline{Y_1}, \cdots, \overline{Y_m})$ =image dans $\Gamma(W)$ de $F(Y_1, \cdots, Y_m) \in I(W)$. Donc $F(\varphi(x)) = 0$. Donc $\varphi(x) \in W$. D'òu la surjectivité. □

Corollaire 2.7.3. *Soit $\varphi : V \to W$ un morphisme d'espaces algébriques affines. Alors φ est un isomorphisme ssi φ^* est un isomorphisme. Donc V et W sont isomorphes ssi $\Gamma(V)$ et $\Gamma(W)$ sont isomorphes.*

Soit $\varphi : V \to W$ un morphisme d'espaces algébriques affines. On dit que φ est dominant si $\overline{\varphi(V)}$ (adhérence pour la topologie de Zariski, ou encore adhérence de Zariski de V) est égale à W, i.e. $\varphi(V)$ est dense dans V.

Proposition 2.7.4. *φ est dominant ssi φ^* est injectif.*

Démonstration. Supposons φ dominant et $f \in \ker(\varphi^*)$, c'est à dire $f \circ \varphi = 0$. Donc $f = 0$ car f continue et $\overline{\varphi(V)} = W$. Donc φ^* est injectif. Considérons $\overline{\varphi(V)}$, c'est un ensemble algébrique affine$\subset W$. Si $\overline{\varphi(V)} \neq W$, il existe $f \in \Gamma(W)$ telle que $f \neq 0$ et $f_{\overline{\varphi(V)}} = 0$. Alors $f \circ \varphi = \varphi^*(f) = 0$. Absurde car φ^* injective. □

Proposition 2.7.5. *Si φ est dominant et V est irréductible, alors W est irréductible.*

Démonstration. Supposons $W = F_1 \cup F_2$, avec F_1, F_2 fermés. On a $V = \varphi^{-1}(W) = \varphi^{-1}(F_1) \cup \varphi^{-1}(F_2)$. Comme $\varphi^{-1}(F_1)$ et $\varphi^{-1}(F_2)$ sont fermés, et V est irréductible, on a $V = \varphi^{-1}(F_1)$ ou $V = \varphi^{-1}(F_2)$. Disons $V = \varphi^{-1}(F_1)$. Alors $\overline{\varphi(V)} = W = \overline{F_1} = F_1$. □

Un anneau A est dit réduit si 0 est son seul élément nilpotent, c'est à dire $\sqrt{0} = \{0\}$. De même, on parle d'algèbre réduite. Si A est un anneau, $A/\sqrt{0}$ est un anneau réduit. Si I est un idéal de A, A/I est réduit ssi $I = \sqrt{I}$.

Toute $K-$algèbre de type fini réduite est isomorphe à une $K-$algèbre de la forme $K[X_1, \cdots, X_n]/I$ où I est un idéal radical.

Théorème 2.7.6. *Supposons K algébriquement clos. Le foncteur Γ est une équivalence de catégories entre les espaces algébriquements affines et les $K-$algèbres de type fini réduites.*

Remarques 2.7.7. *les morphismes de la première catégorie sont les applications régulière, les morphismes de la deuxième catégorie sont les morphismes de $K-$algèbres.*

Démonstration. On a vu que le foncteur Γ est pleinement fidèle. Il reste à voir qu'il est essentiellement surjectif. Soit $A = K[X_1, \cdots, X_n]/I$ un $K-$algèbre de type fini réduite. Alors $I = \sqrt{I}$. On a $V = V(I)$ et $I = \sqrt{I} = I(V)$ (d'après le Nullstellensatz qui s'applique au K algébriquement clos). Donc A est isomorphe à $\Gamma(V)$. Donc le foncteur Γ est essentiellement surjectif. □

Soit V un ensemble algébriquement affine irréductible. Alors $\Gamma(V)$ est un idéal premier. Donc $\Gamma(V)$ est un anneau intègre. Son corps des fonctions $K(V) = \text{Frac}(\Gamma(V))$ est le corps des fonctions rationnelles de V.

2.8 Anneaux gradués

Soit A un anneau (vu comme une $K-$algèbre). On dit que c'est un anneau gradué ou une $K-$algèbre gradué si on a une décomposition $A = \bigoplus_{n\in\mathbb{N}} A_n$ où A_n groupe ou $K-$espace vectoriel avec $A_n A_m \subset A_{n+m}$ pour n, m entiers≥ 0. Les éléments de A_n sont homogènes de degré n. Alors A_0 est un sous-anneau ou une sous $K-$algèbre de A on pose $A^+ = \bigoplus_{n>0} A_n$. C'est un idéal de A. On a $A/A^+ \simeq A_0$.

Exemples 2.8.1. $A = K[X_1, \cdots, X_n]$, en posant A_k =engendré par $X_1^{d_1} \cdots X_r^{d_r}$ avec $d_1 + \cdots + d_r = k$ (choix arbitaire). Alors, $A_0 = k$, A^+ =polynômes sans terme constant.

Proposition 2.8.2. *Soit A une $K-$algèbre graduée ou un anneau gradué. Soit $I \subset A$ un idéal. Alors I est engendré par des éléments homogènes ssi pour tout $P \in I$ avec $P = \sum_{n\in\mathbb{N}} P_n$ avec $P_n \in A_n$, on a $P_n \in I$ pour tout $n \in N$.*

Démonstration. Supposons I engendré par des éléments homogènes (l'autre sens est évident). Posons $I = (Q_1, \cdots, Q_n)$ avec $Q_1, \cdots, Q_r$ homogènes $Q_i \in A_{d_i}$. Soit $P \in I$. Posons $P = \sum_{n\in\mathbb{N}} P_n$ avec $P_n \in A_n$. On peut écrire $P = \sum_j R_j Q_j$ avec $R_j \in A$. Examinons le terme de j plus haut degré. On a $P_r = \sum_j R_{j,r-d_j} Q_j$ où $R_{j,r-d_j}$ est la partie de degré $r - d_j$ de R_j. Par récurrence descendente, on a $P_n \in I$ pour tout n. □

Soit I un idéal homogène de l'ensemble (ou $K-$algèbre) gradué A. Alors A/I est un anneau (ou une $K-$algèbre) gradué.

Proposition 2.8.3. *Soit I un idéal homogène de l'anneau (ou $K-$algèbre) gradué A. Alors $\sqrt{I}$ est un idéal homogène.*

Démonstration. Soit $P \in \sqrt{I}$. Posons $P = \sum_{n\in\mathbb{N}}$ avec $P_n \in A_n$. Soit P_d le terme de plus haut degré. Il existe k entier≥ 1 tel que $P^k \in I$. Le terme de plus haut degré de P^k est P_d^k. Comme I est homogène, $P_d^k \in I$. Donc $P_d \in \sqrt{I}$. Par récurrence descendente, on montre que $P_n \in \sqrt{I}$ pour tout n. □

2.9 Ensemble algébrique projectif

Soit n un entier≥ 0. Soit K un corps. Soit E un $K-$espace vectoriel de dimmension $n+1$. Sur E on considère la relation d'équivalence $\sim$ donnée par $x \sim y$ ssi il existe $\lambda \in K^{\times}$ tel que $x = \lambda y$. Ses classes sont les droites privés de 0 de E.

On pose $\mathbb{P}(E) = {}^{E-\{0\}}/_{\sim}$. C'est l'espace projectif associé à E. Si $E = K^{n+1}$, on pose $\mathbb{P}^n(K) = \mathbb{P}(E)$. C'est l'espace projectif standard. Si F est un sous-$K-$espace vectoriel de E, on a $\mathbb{P}(F) \subset \mathbb{P}(E)$. C'est un sous-espace projectif de $\mathbb{P}(E)$.

Si V et W sont des sous-espaces vectoriels de E de dimensions $r+1$ et $s+1$ respectivement, alors $V \cap W$ est un sous-espace projectif de dimension$\geq r+s-n$ (La dimension de $\mathbb{P}(E)$ est n). Pour $n = 1$, on parle de la droite projective. Pour $n = 2$, on parle du plan projectif. Le groupe linéaire $GL(E)$ opère sur E. Cette action passe quotient $\mathbb{P}(E)$ et se factorise par $GL(E)/\Delta = PGL(E)$ où $\Delta = \{homothties\ de\ E\}$ (de la forme $x \mapsto \lambda x$ avec $\lambda \in K^{\times}$). Le groupe $PGL(E)$ s'appelle le groupe projectif linéaire. L'action de ses éléments s'appellent des homographies. Pour $E = K^2$ et $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(E)$. On a $g(u,1) = (au+b, cu+d)$. Dans $\mathbb{P}(E)$, on a $g(u,1) = \Big(\underbrace{\frac{au+b}{cu+d}}_{homographie}, 1 \Big)$. Soit $x = (x_0, x_1, \cdots, x_n) \in K^{n+1}\backslash\{0\}$. Si on choisit une base de E, on a un isomorphisme $K^{n+1} \simeq E$ et donc $\mathbb{P}^n(K) \simeq \mathbb{P}(E)$. Soit H l'hyperplan de K^{n+1} donné par $H = \{(x_0, x_1, \cdots, x_n) | x_0 = 0\}$. Notons $\overline{H}$ l'image de H dans $\mathbb{P}^n(K)$. Posons $U = \mathbb{P}^n(K) - \overline{H}$. On peut identifier U à K^n par $\bar{x} = (x_0, x_1, \cdots, x_n)$ associe $\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}, \cdots, \frac{x_n}{x_0}\right)$. De plus, on peut identier $\overline{H}$ à $\mathbb{P}^{n-1}(K)$ (en choisissant une base de H). On a $\mathbb{P}^n(K) \simeq K^n \cup \mathbb{P}^{n-1}(K)$, ici $\overline{H} \simeq \mathbb{P}^{n-1}(K)$ est l'hyperplan à l'infini. En particulier, $\mathbb{P}^1(K) \simeq K \cup \{point\ à\ l'infini\} \simeq K \cup \{\infty\}$.

Soit $P \in K[X_0, X_1, \cdots, X_n]$ (vu comme $K-$algèbre graduée). Posons $P = P_0 + \cdots + P_k$ avec $P_0, \cdots, P_k$ homogènes. Soit $\bar{x} \in \mathbb{P}^n(K)$ de coordonnées homogènes $(x_0, \cdots, x_n)$. Alors, $\bar{x}$ est un zéro de P ssi on a $P(\lambda x_0, \lambda x_1, \cdots, \lambda x_n) = 0$ pour tout $\lambda \in K^n$. Comme $P_i(\lambda x_0, \lambda x_1, \cdots, \lambda x_n) = \lambda^i P_i(x_0, \cdots, x_n)$, cela revient à dire $\sum_{i=0}^{k} \lambda^i P_i(x_0, \cdots, x_n) = 0$ pour tout $\lambda \in K^{\times}$. Supposons K infini. Cela entraîne $P_i(x_0, \cdots, x_n) = 0$ pour tout i, $0 \leq i \leq k$. Soit $S \subset K\{X_0, X_1, \cdots, X_n\}$. On pose $V_p(S) = \{x \in \mathbb{P}^n(K) \mid F(x) = 0\ pour\ tout\ F \in S\}$. C'est l'ensemble algébrique projectif associé à S. On peut supposer S fini (car l'anneau

$K[X_0, \cdots, X_n]$ est noethérien) et formé de polynômes homogènes.

On a $V_p(\varnothing) = \mathbb{P}^n$, $V_p(K[X_0, \cdots, X_n]^+) = \varnothing$. Pour x de coordonnées homogènes $(x_0, \cdots, x_n)$ avec $x_0 \neq 0$, on a $\{x\} = V_p(X_1 - X_1X_0, X_2 - X_2X_0, \cdots, X_n - X_nX_0)$. L'application $S \to V_p(S)$ est décroissante. L'espace projectif $\mathbb{P}^n(K)$ est muni de la topologie de Zariski dont les ouverts sont les complémentaires des ensembles algébriques projectifs. Elle induit la topologie de Zariski de $K^n \subset \mathbb{P}^n(K)$.

Pour $V \subset \mathbb{P}^n(K)$, on pose $I_p(V) = \{P \in K[X_1, \cdots, X_n] \mid P(x) = 0 \textit{ pour tout } x \in V\}$. C'est un idéal radical et homogène de $K[X_0, \cdots, X_n]$. L'application $V \mapsto I_p(V)$ est décroissante. On a $V_p(I_p(V)) = V$ et $I \subset I_p(V_p(I))$. On a $I_p(P) = 0$, $I_p(\varnothing) = K[X_0, \cdots, X_n]$. Notons d'irréductible pour la topologie de Zariski.

Le cône de V est noté $C(V)$. C'est

$C(V) = \{(x_0, \cdots, x_n) \in K^{n+1} \mid (x_0, \cdots, x_n) \textit{ est coordonne homogène d'un élément de } V\}$.

Théorème 2.9.1. *(Nullstellensatz projectif) On suppose K algébriquement clos. Soit I un idéal homogène de $K[X_0, \cdots, X_n]$.*

1. *On a $V_p(I) = \varnothing$ ssi il existe k entier≥ 0 tel que $(X_0, \cdots, X_n)^k \subset I$ ssi $(X_0, \cdots, X_n) = K[X_0, \cdots, X_n]^+ \subset \sqrt{I}$;*
2. *Si $V_p(I) \neq \varnothing$, on a $I_p(V_p(I)) = \sqrt{I}$.*

Démonstration. Si $I = K[X_0, \cdots, X_n]$, on a $V_p(I) = \varnothing$ et 1. est vérifié. Si $I \subsetneqq K[X_0, \cdots, X_n]$. On considère la cône de $V_p(I)$. On a $C(V_p(I)) \subset K^{n+1}$. De plus $C(V_p(I)) = V(I)$ par le Nullstellensatz affine. On a $V(I) \neq \varnothing$ ssi $C(V_p(I)) = \{0\}$, c'est à dire $\sqrt{I} = K[X_0, \cdots, X_n]^+$. On a réduit 1.

Si $V_p(I) = \varnothing$, on a $I_p(V_p(I)) = I(C(V_p(I))) = \sqrt{I}$ d'après le Nullstellensatz.

Pour résumer, les ensembles algébriques projectifs de $\mathbb{P}^n(K)$ correspondents aux idéaux homogènes radicaux$\neq (X_0, \cdots, X_n)$.

On pose $\Gamma_h(V) = K[X_0, \cdots, X_n]/I_p(V)$ $K-$algèbre graduée quotiente. □

2.10 Faisceaux

Soit X un espace topologique. Soit E un ensemble. Un faisceau de fonctions à valeurs dans E est une loi que à un ouvert U de X associe $\mathcal{F}(U) \subset \{fonction\ U \to E\}$, telle que

1. Pour tout V ouvert$\subset U$ et tout $f \in \mathcal{F}(U)$ on a $f|_V \in \mathcal{F}(V)$; (propriété de restriction)
2. Si $(U_i)_{i\in I}$ est une famille d'ouverts de X telle que $U = \bigcup_{i\in I} U_i$ (recouvrement de U), et $(f_i)_{i\in I}$ avec $f_i \in \mathcal{F}(U_i)$ avec pour tout $i, j \in I$ on a $f_i|_{U_i\cap U_j} = f_j|_{U_i\cap U_j}$, alors il existe un unique $f \in \mathcal{F}(U)$ telle. que pour tout $i \in I$, $f|_{U_i} = f_i$. (propriété de recollement)

Exemple 2.10.1.

$$\mathcal{F}(U) = \{fonctions\ continues\ U \to E\}.$$

On peut remplacer continue par différentiable, analytiques, polynomiales... Beaucoup de choix.

On note $r_{V,U} : \mathcal{F}(U) \to \mathcal{F}(V)$ la restriction. On a $r_{W,V} \circ r_{V,U} = r_{W,U}$ et $r_{U,U} = id_{\mathcal{F}(U)}$ pour U, V, W ouverts de X avec $W \subset V \subset U$. On pose $\mathcal{F}(U) = \Gamma(U, \mathcal{F}) = \{sections\ de\ \mathcal{F}\ sur\ U\}$. Si $X = U$, $\mathcal{F}(X)$ est l'ensemble des sections globales de $\mathcal{F}$.

Un préfaisceau sur X est une loi qui a un ouvert U de X associe un ensemble $\mathcal{F}(U)$ avec pour tout ouvert $V \subset U$ on a $r_{V,U} : \mathcal{F}(U) \to \mathcal{F}(V)$ et qui vérifie $r_{W,V} \circ r_{V,U} = r_{W,U}$ pour tous $W \subset V \subset U$ et $r_{U,U} = id_{\mathcal{F}(U)}$ pour tous $W \subset V \subset U$ (ouverts de X).

C'est un faisceau si de plus on a la propriété de recollement : si $U = \left(\bigcup_{i\in I} U_i\right)$ (recouvrement) et $f_i \in \mathcal{F}(U_i)$ tels que $r_{U_i\cap U_j,U_i}(f_i) = r_{U_i\cap U_j,U_j}(f_j)$ pour tout $i, j \in I$. Il existe un unique $f \in \mathcal{F}(U)$ tel que pour tout $i \in I$ on a $r_{U_i,U}(f) = f_i$.

Remarques 2.10.2.

1. *Inventé par Jean Leray (1906-1998) ;*
2. *Si $\mathcal{G}$ est un faisceau sur X et que $\mathcal{G}(U) \subset \mathcal{F}(U)$, on dit que $\mathcal{G}$ est un sous-faisceau ;*
3. *On a un préfaisceau des fonctions constantes. Ce n'est pas un faisceau si X n'est pas constantes ;*
4. *Tout faisceau est un faisceau de fonctions. Soit $P \in X$. Posons $E_p = \{(U, s) \mid U\ ouvert \subset X,\ P \in U,\ s \in \mathcal{F}(U)\}$. On a une relation d'équivalence $\sim$ sur E_p donnée par $(U, s) \sim (V, t)$ ssi il existe W ouvert$\subset U\cap V$ tel que $s|_W = t|_W$. (on note $r_{W,U}(s) = s|_W$) La classe de (U, s) pour cette relation s'appelle le germe de s en P. On pose $\mathcal{F}_P = \{germes\ en\ P\}$ la fibre de $\mathcal{F}$ en P. On pose $E = \bigsqcup_{P\in X} \mathcal{F}_P$. Alors on pose $i_U : F(U) \to \{fonctions\ U \to E\}$. Donc $\mathcal{F}$ est un sous-faisceau du faisceau des fonctions $X \to E$;*

5. $X = \mathbb{C}$, $\mathcal{F}(U) = \left\{ \begin{smallmatrix} fonctions\ holomorphes \\ bornée\ sur\ U \end{smallmatrix} \right\}$, $\Gamma(\mathbb{C}, \mathcal{F}) = \{fonctions\ constantes\}$.

Proposition 2.10.3. *Soit $\mathcal{F}$ un préfaisceau de fonctions sur X. Posons, pour U ouvert de X*

$$\mathcal{F}^+(U) = \left\{ f : U \to E \;\middle|\; \begin{array}{c} pour\ tout\ x \in U,\ il\ existe\ un\ ouvert\ V\ avec \\ x \in V \subset U,\ et\ q \in \mathcal{F}(V)\ tel\ que\ f|_V = q \end{array} \right\}.$$

Alors $\mathcal{F}^+$ est un faisceau sur X. C'est le faisceau associé à $\mathcal{F}$ (plus petit faisceau contenant $\mathcal{F}$).

En général, si $\mathcal{F}$ est un faisceau, $\mathcal{F}(U)$ a une structure algébrique : groupe abélien, module, anneau, $K-$algèbre, etc... $\mathcal{F}(U)$ est dans une catégorie, $r_{V,U}$ est un morphisme de cette catégorie.

Un espace annelé est un espace topologique muni d'un faisceau d'anneaux : $\mathcal{F}(U)$ est un anneau, $r_{V,U}$ est un morphisme d'anneaux. On se limite à la situation suivante :

Soit k un corps algébriquement clos. On considère des faisceaux de $K-$algèbres de fonctions à valeurs dans K. Soit X un espace annelé, on note $\mathcal{O}_X$ le faisceau d'anneaux associé. C'est le faisceau structural sur X. On note $(X, \mathcal{O}_X)$ l'espace annelé. Soient $(X, \mathcal{O}_X)$ et $(Y, \mathcal{O}_Y)$ des espaces annelés, un morphisme d'espaces annelés est une application continue $\varphi : X \to Y$ et telle que pour tout ouvert U de Y et tout $g : U \to K$ avec $g \in \Gamma(U, \mathcal{O}_Y)$, on a $g \circ \varphi \in \Gamma(\varphi^{-1}(U), \mathcal{O}_X)$ (si $\mathcal{O}_X$ et $\mathcal{O}_Y$ sont des faisceaux de fonctions). En général, il faut pour tout U ouvert de Y, $\varphi_U^* : \Gamma(U, \mathcal{O}_Y) \to \Gamma(\varphi^{-1}(U), \mathcal{O}_X)$ avec $r_{\varphi^{-1}(V),\varphi^{-1}(U)} \circ \varphi_U^* = \varphi_V^* \circ r_{V,U}$ pour tous U, V ouverts de Y.

2.11 Localisation

"Local"="près d'un point" en géométrie (et en topologie) mais aussi en algébrique. Soit A un anneau. Soit $S \subset A$. On dit que S est un ensemble multiplicatif si $1 \in S$ et pour tout $s_1, s_2 \in S$ on a $s_1 s_2 \in S$.

Supposons S multiplicatif. L'anneau quotient (ou anneau de fractions) de A par S est $A \times S/\sim$ où $\sim$ est la relation suivante sur $A \times S$: On a $(a, s) \sim (a', s')$ ssi il existe $u \in S$ tel que $u(as' - a's) = 0$. La relation $\sim$ est d'équivalence. La classe de (a, s) est notée $\frac{a}{s}$. On

note $S^{-1}A$ ou A_S l'ensemble quotient. Il est muni d'une addition et d'une multiplication par $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$ et $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$. Notons $\frac{0}{1}$ est le neutre par $+$, et $\frac{1}{1}$ est le neutre par $\times$.

Soient $a, a', b, b' \in A$, $s, s', t, t' \in S$ tels que $\frac{a}{s} = \frac{a'}{s'}$ et $\frac{b}{t} = \frac{b'}{t'}$. Il existe $u, v \in S$ tel que $u(as' - a's) = 0$, $v(bt' - b't) = 0$. Donc $vtt'u(as' - a's) = 0$, $uss'v(bt' - b't) = 0$ et alors $uv(tt'(as' - a's) + ss'(bt' - b't)) = 0$. Donc $\frac{as'-a's}{ss'} = -\frac{bt'-b't}{tt'}$ et $\frac{at+bs}{st} = \frac{a't'+b's'}{s't'}$ (à vérifier). Donc $+$ bien défini. De même pour $\times$.

On montre que $(S^{-1}A, +, \times)$ est un anneau. On a un morphisme d'anneaux $\begin{array}{c} \varphi_S : A \longrightarrow S^{-1}A \\ a \mapsto a/1 \end{array}$.
De plus $\varphi_S(S) \subset (S^{-1}A)^\times$ car pour $s \in A$, on a $\varphi_S(s) = \frac{s}{1} = \left(\frac{1}{s}\right)^{-1}$.

Si S contient un diviseur de 0, on a $S^{-1}A = \{0\}$.

On a fixé A et S. Considérons la catégorie $\mathcal{C}$ dont les objets sont les morphismes d'anneaux $f : A \to B$ tels que $f(S) \subset B^\times$. Pour $f, f' \in \mathcal{O}b(\mathcal{C})$, un morphisme d'anneaux $g : B \to B'$ tel que

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow^{f'} & \downarrow g \\ & & B' \end{array}$$

commute, i.e. $g \circ f = f'$. Alors $\varphi_S : A \to S^{-1}A$ est un objet initial. Pour tout $f \in \mathcal{O}b(\mathcal{C})$, il existe un unique morphisme d'anneaux $S^{-1}A \to B$ avec

$$\begin{array}{ccc} A & \xrightarrow{\varphi_S} & S^{-1}A \\ & \searrow^{f} & \downarrow g \\ & & B \end{array}$$

commute.

Si A est intègre et $0 \notin S$, $\varphi_S : A \to S^{-1}A$ est injective. En effet si $\varphi_S(a) = 0$ on a $\frac{a}{1} = \frac{0}{1}$ et donc il existe $u \in S$ tel que $u(a - 0) = ua = 0$. Les idéaux premiers de $S^{-1}A$ correspondent aux idéaux premier de A ne rencontrant pas S.

Cas particuliers :

1. Si $S = A^\times$, on a $S^{-1}A = A$;
2. Si A est intègre et $S = A\backslash\{0\}$, on a $S^{-1}A = \mathrm{Frac}A$ corps des fractions de A ;
3. Si $S = A - \mathfrak{p}$ où $\mathfrak{p}$ est un idéal premier, on obtient $S^{-1}A = A_\mathfrak{p}$ (notation). C'est le localisé de A en $\mathfrak{p}$. C'est un anneau local. (qui n'a qu'un seul idéal maximal). L'idéal maximal de $A_\mathfrak{p}$ est $\mathfrak{p}A_\mathfrak{p} = \{\frac{a}{s} \mid a \in \mathfrak{p}, s \in S\}$ et $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \simeq rmFrac(A/\mathfrak{p})$;
4. Si $S = A\backslash\{diviseurs\ de\ 0\ dans\ A\}$, $S^{-1}A$ s'appelle l'anneau total des fractions de A ;
5. Si $f \in A$, on peut considérer $S = \{1, f, \cdots, f^n, \cdots\}$. Alors $S^{-1}A \simeq A[T]/(fT - 1)$.

Proposition 2.11.1. *Soit I un idéal de A. On a $\sqrt{I}S^{-1}A = \sqrt{IS^{-1}A}$.*

Démonstration. On a $\sqrt{I}S^{-1}A \subset \sqrt{IS^{-1}A}$. Réciproquement, soit $\frac{x}{s} \in \sqrt{IS^{-1}A}$ avec $x \in A$, $s \in S$. Il existe un entier$n \geq 1$ tel que $\left(\frac{x}{s}\right)^m = \frac{y}{t}$ avec $y \in I$ et $t \in S$. Il existe $u \in S$ tel que $u(tx^m - s^n y) = 0$. Donc $utx^m = us^n y$ et $usy^n \in I$. Donc $utx^m \in I$ et alors $(utx)^m \in I$. Donc $\frac{x}{s} = \frac{utx}{uts} \in \sqrt{I}S^{-1}A$. □

Variante : on peut appliquer cette construction à un $A-$module M.

Soit M un $A-$module. On définit une relation d'équivalence $\sim$ sur $M \times S$ par $(m, s) \sim (m', s')$ ssi il existe $u \in S$ tel que $u(s'm - sm') = 0$. On note $S^{-1}M$ ou M_S l'ensemble quotient. C'est un $S^{-1}A-$module. On note $\frac{m}{s}$ la classe de (m, s). On a une addition par passage au quotient et une structure de $S^{-1}A-$module donnée par $\frac{a}{t} \cdot \frac{t}{s} = \frac{am}{st}$. (Comme on a $\varphi_S : A \to A_S$), $S^{-1}M$ est ainsi un $A-$module. On a un morphisme de $A-$modules $M \to S^{-1}M$, $m \to \frac{m}{1}$. En particulier, si I est un idéal de A, on a $S^{-1}I$ s'identifie à $IS^{-1}A = \{\frac{a}{s} \in S^{-1}A \mid a \in I,\ s \in S\}$. (localisé de I en S). De même $S^{-1}M$ est le localisé de M en S.

La saturation de I par S et $\varphi_S^{-1}(S^{-1}I) = \{a \in A \mid il\ existe\ s \in S\ avec\ as \in I\}$. C'est un idéal de A.

Revenons au localisé du module M. Considérons la catégorie $\mathcal{C}$ dont les objets sont les morphismes $F : M \to N$ où N est un $B-$module et on a $f : A \to B$ telle que $f(S) \subset B^\times$ et f morphisme d'anneaux (donc $N : A-$module) tel que F est un morphisme de $A-$module. On note (f, F) un tel objet. Soient (f, F), $(f, F') \in \mathcal{O}b(\mathcal{C})$. Un morphisme de (f, F) vers (f', F') est un morphisme d'anneaux $g : B \to B'$ et $G : N \to N'$ un morphisme de $B-$modules tels que les diagrammes

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow^{f'} & \downarrow g \\ & & B' \end{array} \qquad \begin{array}{ccc} M & \xrightarrow{F} & N \\ & \searrow^{F'} & \downarrow G \\ & & N' \end{array}$$

commutent.

Soit (f, F) un objet de $\mathcal{C}$. Il existe un unique morphisme d'anneaux $S^{-1}A \to B$ et un unique morphisme de $S^{-1}A-$modules $S^{-1}M \to N$ tels que les diagrammes

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow^{f'} & \downarrow g \\ & & B' \end{array} \qquad \begin{array}{ccc} M & \xrightarrow{F} & N \\ & \searrow^{F'} & \downarrow G \\ & & N' \end{array}$$

commutent. (C'est la propriété universelle du localisé)

Autre construction de $S^{-1}M$. On peut considérer $M \otimes_A S^{-1}A$. En effet $S^{-1}A$ est un $A-$module car $a \cdot \frac{b}{s} = \frac{ab}{s}$. (action de A sur $S^{-1}A$) Donc $M \otimes_A S^{-1}A$ est un $S^{-1}A-$module. On a

$$\begin{aligned} M &\longrightarrow M \otimes_A S^{-1}A \\ m &\longmapsto m \otimes_A 1. \end{aligned}$$

(morphisme de $A-$module) Donc il existe un unique morphisme de $S^{-1}A-$modules

$$\begin{aligned} S^{-1}M &\longrightarrow M \otimes_A S^{-1}A \\ \frac{m}{s} &\longmapsto m \otimes_A \frac{1}{s}, \end{aligned}$$

dont la réciproque est $m \otimes \frac{x}{s} \mapsto \frac{xm}{s}$. Donc $S^{-1}M$ est isomorphe à $M \otimes_A S^{-1}A$. On a défini un foncteur de la catégorie des $A-$modules vers la catégorie des $S^{-1}A$modules.

2.12 Le faisceau structural d'un ensemble algébrique affine

Soit K un corps algébriquement clos, soit n un entier≥ 1. Soit V un ensemble algébrique affine contenu dans K^n. Quelles fonctions sur V ?

La topologie de Zariski sur V a pour base les $D(f) = \{x \in V \mid f(x) \neq 0\}$ pour $f \in \Gamma(V)$ (ouvert standard).

Proposition 2.12.1. *Soit X un espace topologique. Soit $\mathcal{B}$ une base d'ouverts de X. Soit E un ensemble. Supposons que pour $U \in \mathcal{B}$, on a $\mathcal{F}(U) \subset \{fonctions\ U \to E\}$ tel que*

1. *Si $V, U \in \mathcal{B}$ avec $V \subset U$ et $s \in \mathcal{F}(U)$, on a $s|_V \in \mathcal{F}(V)$.*
2. *Soit $U \in \mathcal{B}$ tel qu'il existe $(U_i)_{i\in I}$, $U_i \in \mathcal{B}$ avec $U = \bigcup_{i\in I} U_i$ et $s : U \to E$ telle que pour tout $i \in I$, on a $s|_{U_i} \in \mathcal{F}(U_i)$, alors $s \in \mathcal{F}(U)$.*

Alors il existe un unique faisceau $\overline{\mathcal{F}}$ sur X de fonctions dans E tels que pour tout $U \in \mathcal{B}$, on a $\overline{\mathcal{F}}(U) = \mathcal{F}(U)$.

Démonstration. Soit U un ouvert de X. Il existe $(U_i)_{i\in I}$ avec $U_i \in \mathcal{B}$ tel que $U = \bigcup_{i\in I} U_i$. On pose

$$\overline{\mathcal{F}}(U) = \{s : U \to E \mid s|_{U_i} \in \mathcal{F}(U_i),\ \forall i\}.$$

C'est indépendant du recouvrement de U choisi. En effet, soit $U = \bigcup_{i\in I} U_i = \bigcup_{j\in J} V_j$ avec $U_i, V_j \in \mathcal{B}$. Soit $s : U \to E$ telle que $s|_{U_i} \in \mathcal{F}(U_i),\ \forall i$. Alors $s|_{U_i\cap V_j} = (s|_{U_i})|_{U_i\cap V_j} \in \mathcal{F}(V_j)$ à cause de 1. .Comme $V_j = \bigcup_{i\in I} U_i \cap V_j$, on a $s|_{V_j} \in \mathcal{F}(V_j)$ à cause de 2. .

Soit $X = \bigcup_i U_i$ avec les U_i ouverts. Soit $s : X \to E$ telle que $s|_{U_i} \in \overline{\mathcal{F}}(U_i)$. On peut choisir les $U_{i,j} \in \mathcal{B}$ tel que $U_i = \bigcup_j U_{i,j}$ pour tout i et $(s|_{U_i})|_{U_{i,j}} \in \mathcal{F}(U_{i,j})$ pour tout i, j. Alors $X = \bigcup_{i,j} U_{i,j}$, et $s|_{U_{i,j}} = (s|_{U_i})|_{U_{i,j}} \in \mathcal{F}(U_{i,j})$ pour tout i, j. Cela donne que $s \in \overline{\mathcal{F}}(X)$.

Pour l'unicité, soit $\mathcal{G}$ un autre faisceau satisfaisant les hypothèses. Soit $U \subset X$ ouvert. Soit $U = \bigcup_{i\in I} U_i$ avec $U_i \in \mathcal{B}$. Pour tout $s \in \mathcal{G}(U)$, $i \in I$, on a $s|_{U_i} \in \mathcal{G}(U_i) = \mathcal{F}(U_i)$. Donc $s \in \overline{\mathcal{F}}(U)$ par définition. Et, par la définition de faisceau (recollement), on a $\overline{\mathcal{F}}(U) \subset \mathcal{G}(U)$. □

Pour défini un faisceau sur V, il suffit de défini $\mathcal{F}(U)$ pour U ouvert standard et de vérifier 1. et 2. .

Corollaire 2.12.2. *Soit X un espace topologique. Soit $\mathcal{B}$ une base d'ouverts de X. Soit $\mathcal{F}$ un faisceau sur X. Soit $\mathcal{G}$ un préfaisceau sur X. Si, pour tout $U \in \mathcal{B}$, on a $\mathcal{F}(U) = \mathcal{G}(U)$, alors on a $\mathcal{F} = \mathcal{G}^+$ (faisceau associé à $\mathcal{G}$).*

Démonstration. Le faisceau $\mathcal{G}^+$ coïncide avec $\mathcal{F}$ sur $\mathcal{B}$ et donc partout par la proposition précédente. □

Il faut déterminer $\Gamma(D(f), \mathcal{O}_V)$ pour $D(f)$ ouvert standard. On veut $f^{-1} \in \Gamma(D(f), \mathcal{O}_V)$

Lemme 2.12.3. *Soit $\rho : \Gamma(V)_f \to \{fonction\ D(f) \to K\}$. C'est une application injective.*

Démonstration. Ici $\Gamma(V)_f$ =anneau de fraction de $\Gamma(V)$ par $S = \{f^n,\ n \geq 0\}$. Soit $\frac{g}{f^n} \in \Gamma(V)_f$ tel que $\rho\left(\frac{g}{f^n}\right) = 0$. Alors $\frac{g}{f^n}\Big|_{D(f)} = 0$. Donc $g|_{D(f)} = 0$ et de plus $fg = 0$ sur V, on a $\frac{g}{f^n} = 0$ dans $\Gamma(V)_f$. □

On pose $\Gamma(D(f), \mathcal{O}_V) = \Gamma(V)_f$ vu comme $\subset \{fonction\ D(f) \to K\}$. Pour vérifier que cela définit un faisceau, il faut vérifier 1. et 2. . Ce faisceau est le faisceau des fonctions régulières sur V.

Proposition 2.12.4. *Pour $D(f)$ parcourant les ouverts standards, $\mathcal{F}(D(f), \mathcal{O}_V)$ satisfait les propriétés de restriction 1. et de recollement 2.*

Démonstration. Vérifions 1. . Soient $f, g \in \Gamma(V)$ telles que $D(f) \subset D(g)$. On a $V(g) \subset V(f)$. Alors $f|_{V(g)} = 0$. D'après le Nullstellensatz il existe n entier≥ 1 tel que $f^n = gh$ avec $h \in K[X_1, \cdots, X_n]$. Soit $\frac{u}{g^i} \in \Gamma(V) = \mathcal{F}(D(g), \mathcal{O}_V)$ on a $\frac{u}{g^i} = \frac{uh^i}{g^i h^i} = \frac{uh^i}{f^{ni}} \in \Gamma(V)_f$. On a bien la restriction.

Vérifions 2. . Soit $f \in \Gamma(V)$. Soit $(f_i)_{i\in I}$, $f_i \in \Gamma(V)$ telle que $D(f) = \bigcup_{i\in I} D(f_i)$ avec $f_i \neq 0$. Donc $V(f) = \bigcap_{i\in I} V(f_i) = V$ (idéal engendré par $(f_i)_{i\in I}$). Comme $K[X_1, \cdots, X_n]$ est noethérien, on peut supposer I fini.

Soit $s_i \in \mathcal{F}(D(f_i), \mathcal{O}_V) = \Gamma(V)_{f_i}$. On pose $s_i = \frac{u_i}{f_i^n}$ (on peut supposer n indépendant de i car I est fini et $\frac{u_i}{f_i^{n_i}} = \frac{u_i f_i^{n-n_i}}{f_i^n}$). On suppose que $s_i|_{D(f_i)\cap D(f_j)} = s_j|_{D(f_i)\cap D(f_j)}$. Alors il existe t

entier≥ 0 tel que $f_i^t f_j^t(u_i f_j^n - u_j f_i^n) = 0$. De plus $V((f_i)_{i\in I}) = V((f_i^{n+t})_{i\in I})$. Donc il existe m entier≥ 1 tel que

$$f^m = \sum_{i\in I} b_i f_i^{n+t}$$

avec $b_i \in V[X_1, \cdots, X_n]$ (Nullstellensatz). Posons $s = \sum_{j\in I} u_j b_j f_j^t / f^m \in \Gamma(V)_f$. Montons que $s|_{D(f_i)} = s_i = \frac{u_i}{f_i^n}$. On a

$$\begin{aligned} f_i^t(f_i^n \sum_{j\in I} u_j b_j f_j^t) &= \sum_{j\in I} \underbrace{u_j f_i^{n+t} f_j^t}_{=u_i f_j^{n+t} f_i^t} b_j \\ &= u_i f_i^t \sum_{j\in J} b_j f_j^{m+t} \\ &= u_i f_i^t f^m. \end{aligned}$$

Donc $f_i^t(f_i^n \sum_{j\in I} u_j b_j f_j^t - u_i f^m) = 0$. Donc s coïncide avec s_i dans $\Gamma(V)_{f_i}$. Donc on a bien le recollement.

On a bien défini le faisceau structural. □

Remarques 2.12.5. *1. Si $\Gamma(V)$ est intègre (i.e. V est irréductible), on a $\Gamma(V)_f \subset K(V)$ et $\Gamma(V) \to \Gamma(V)_f$ est injective ;*

2. Si $f, g \in \Gamma(V)$ sont telles que $D(f) = D(g)$ il faut vérifier que $\Gamma(V)_f = \Gamma(V)_g$. Cela résulte de la vérification de la propriété de restriction ;

3. En général, ce n'est pas facile de décrire $\mathcal{F}(U, \mathcal{O}_V)$ lorsque U n'est pas un ouvert standard. Par exemple $U = K^2 \backslash \{(0,0)\}$

2.13 Variétés algébrique

Soit K un corps algébriquement clos. Une variété algébrique affine est un espace annelé isomorphe à $(V, \mathcal{O}_V)$ où V est un ensemble algébriquement affine et $\mathcal{O}_V$ est la faisceau des fonctions régulières sur V. Ce sont les objets de la catégorie des variétés algébriques affines, dont les morphismes sont les morphismes d'espaces annelés.

Remarques 2.13.1. *1. Dans certains livres, la définition est différente. On demande que la variété est irréductible ;*

2. On va demander pas que la variété soit contenue dans K^n,

3. *On écrit souvent : "Soit V une variété..." plutôt que "Soit $(V, \mathcal{O}_V)$ une variété...".*

Proposition 2.13.2. *Soient X, Y des variétés algébriques affines. Soit $\varphi : X \to Y$. Supposons que $Y = \bigcup_{i\in I} V_i$, avec V_i ouvert de Y et que $\varphi^{-1}(V_i) = \bigcup_{j\in J} U_{i,j}$ et que $\varphi|_{U_{i,j}} : U_{i,j} \to V_i$ soit un morphisme. Alors φ est un morphisme.*

Démonstration. φ est continue car φ est continue localement. Soit V un ouvert de Y et soit $f \in \Gamma(V, \mathcal{O}_Y)$. On a $f|_{V_i} \in \Gamma(V_i, \mathcal{O}_Y)$. Donc $f|_{V_i} \circ \varphi \in \Gamma(U_{i,j}, \mathcal{O}_X)$ et donc $f \circ \varphi$ est obtenu par recollement. On a bien un morphisme d'espaces annelés. □

Proposition 2.13.3. *Soient X, Y des ensembles algébriques affines. Soit $(X, \mathcal{O}_X)$ et $(Y, \mathcal{O}_Y)$ les variétés algébriques affines associées. On a des bijections*

$$Hom_{\substack{variété\\algébrique}}(X,Y) \simeq Reg_{\substack{fonctions\\régulières}}(X,Y) \simeq Hom_{\substack{K-\\algèbres}}(\Gamma(Y,\mathcal{O}_Y), \Gamma(X,\mathcal{O}_X)).$$

$$\searrow$$

déjà connu

Démonstration. Soit $\varphi \in Hom_{\substack{variété\\algébrique}}(X,Y)$. On a $Y \subset K^m$ pour m entier≥ 1. Posons $\varphi = (\varphi_1, \cdots, \varphi_m)$. On a $\varphi_i = p_i \circ \varphi$ où p_i =projection sur la $i-$ème coordonnée $p_i : Y \to K$. Donc φ est régulière.

Réciproquement, si $\varphi : X \to Y$ est régulière. Soit $D(g)$ un ouvert standard de Y. Soit $f \in \Gamma(D(g), \mathcal{O}_y) = \Gamma(Y)_g$. Posons $f = \frac{h}{g^r}$ avec $r \geq 0$. On a

$$f \circ \varphi = \frac{\varphi^*(h)}{\varphi^*(g)^r} \in \Gamma(D(\varphi^*(g)), \mathcal{O}_X).$$

On a bien un morphisme de variétés algébriques affines. □

La bijection de la proposition établit qu'on a une équivalence de catégorie entre la catégorie des ensembles algébriques affines et la catégorie des variétés algébriques affines.

Définition 2.13.4. Une variété algébrique est un espace annelé quasi compact localement isomorphe à une variété algébriquement affine.

Rappel : Un espace topologique X est dit quasi-compact si pour tout $(U_i)_{i\in I}$ avec U_i ouvert de X et $X = \bigcup_{i\in I} U_i$, il existe $J \subset I$ finie tel que $X = \bigcup_{i\in J} U_i$.

Localement isomorphe signifie que pour tout $x \in$variété algébrique, il existe un ouvert U avec $x \in U$ et tel que U est isomorphe à une variété algébrique affine.

Les variétés algébriques sont les objets de la catégorie des variétés algébriques. Les morphismes sont les morphismes d'espaces annelés. Les ouverts affines sont les ouverts isomorphes à une variété algébrique affine. Par exemple $K^2\backslash\{(0,0)\}$ n'est pas un ouvert affine de K^2.

Proposition 2.13.5. *Soit X une variété algébrique. Les ouverts affines forment une base de la topologie de X.*

Démonstration. On peut écrire $X = \bigcup_{x\in X} U_x$ où U_x est un ouvert affine avec $x \in U_x$. Comme X est quasi-compact, il existe $Z \subset X$, avec Z fini tel que $X = \bigcup_{z\in Z} U_z$. Soit U un ouvert de X. On a $U = \bigcup_{z\in Z}(U_z \cap U)$ réunion d'ouvert affine. Voir proposition suivante. □

Proposition 2.13.6. *Soit V un ensemble algébrique affine. Soit $f \in \Gamma(V)$. Alors $(D(f), \mathcal{O}_{V|D(f)})$ est une variété algébrique affine.*

Démonstration. Supposons $V \subset K^n$. Posons $I = I(V)$. Soit $F \in K[X_1, \cdots, X_n]$ tel que $F|_V = f$. On va réaliser V dans K^{n+1}. Soit

$$\begin{array}{rccc} \varphi : & D(f) & \longrightarrow & K^{n+1} \\ & (x_1, \cdots, x_n) & \longmapsto & (x_1, \cdots, x_n, \dfrac{1}{f(x_1, \cdots, x_n)}). \end{array}$$

On a $Im(\varphi) = V(J)$ où $J \subset K[X_1, \cdots, X_{n+1}]$ donné par $J = I + (X_{n+1}F - 1)$ (astuce de Rabinouitz). Alors φ est un homéomorphisme et $D(f) \simeq V(J)$. De plus $\varphi^{-1}(x_1, \cdots, x_{n+1}) = (x_1, \cdots, x_n)$. On applique le critère des morphismes pour φ et φ^{-1} pour la base des ouverts standards. Pour φ, on écrit $V(J) = \bigcup_i D(h_i)$, on a $\varphi^{-1}(D(h_i)) = D(h_i \circ \varphi)$. □

On applique cette proposition à la proposition précédente.

Proposition 2.13.7. *Soit X une variété algébrique non vide. C'est une réunion finie de fermés irréductibles $\bigcup_{i\in I} F_i$ avec $F_i \not\subset F_j$ si $i \neq j$. De plus de façons unique.*

Lemme 2.13.8. *Soit X un espace topologique. Soit $Y \subset X$. Si Y est irréductible, $\overline{Y}$ est irréductible. On a une correspondance bijective $Y \mapsto \overline{Y}$ et $Z \mapsto Z \cap U$ entre*

$$\left\{ \begin{array}{c} parties\ fermée \\ irréductibles\ Y \subset U \end{array} \right\} \ et \ \left\{ \begin{array}{c} parties\ fermée\ irréductibles \\ Z \subset X\ qui\ rencontrent\ U \end{array} \right\}.$$

Démonstration. Si $\overline{Y} = F_1 \cup F_2$ avec F_1, F_2 fermées de $\overline{Y}$ et donc de X. On a $Y = (F_1 \cap Y) \cup (F_2 \cap Y)$. Donc $Y = F_1 \cap Y$ ou $Y = F_2 \cap Y$ car Y irréductible. Donc $Y = F_1$ ou $Y = F_2$. Donc $\overline{Y} = F_1$ ou $\overline{Y} = F_2$ et alors $\overline{Y}$ est irréductible. □

Démonstration. (de la proposition) On pose $X = \bigcup_{i\in I} U_i$ avec U_i ouvert affine et I fini. Comme chaque U_i est isomorphe à un espace algébrique affine, il s'écrit $U_i = \bigcup_j U_{i,j}$ où $U_{i,j}$ sont irréductibles. On a alors $X = \bigcup_{i,j} \overline{U_{i,j}}$ où $\overline{U_{i,j}}$ adhérence de $U_{i,j}$ dans X. On utilise le lemme précédent, alors $\overline{U_{i,j}}$ est irréductible. □

Soit X une variété algébrique. Soit U un ouvert de X. On le munit de $\mathcal{O}_{X|U}$ qui est un faisceau d'anneaux. Alors $(U, \mathcal{O}_{X|U})$ est une variété algébrique dite sous-variété ouverte de X.

Soit $(X, \mathcal{O}_X)$ une variété algébrique. Soit $Y \subset X$ un fermé. On peut considérer pour V ouvert de Y,

$$\left\{ f : V \to K \;\middle|\; \begin{array}{c} \textit{il existe } U \subset V \textit{ ouvert avec } U \cap Y = V \\ \textit{et il existe } g \in \mathcal{O}_X(U) \textit{ tel que } g|_V = f \end{array} \right\}.$$

C'est un préfaisceau $\mathcal{O}_{0,Y}$ qui n'est pas un faisceau eu général sur Y. Il faut considérer le faisceau associé à $\mathcal{O}_{0,Y}$. On pose

$$\mathcal{O}_Y(V) = \left\{ f : V \to K \;\middle|\; \begin{array}{c} \textit{pour tout } x \in V, \textit{ il existe } U \textit{ ouvert}, \\ x \in U \textit{ et } g \in \mathcal{O}_X(U) \textit{ tel que } g|_{U\cap V} = f|_{U\cap V} \end{array} \right\}.$$

Proposition 2.13.9. *Cela fait de $(Y, \mathcal{O}_Y)$ une variété algébrique (affine si X est affine). De plus, l'inclusion $Y \to X$ est un morphisme.*

Démonstration. En recouvrement X par des variétés affines, on se ramène au cas où X est affine. Il suffit de montrer que $\mathcal{O}_Y$ est le faisceau R_Y des régulières sur Y.

Soit $f \in \Gamma(X)$ d'image $\bar{f}$ dans $\Gamma(Y)$. Il suffit de prouver que $R(D(\bar{f})) = \mathcal{O}_{0,Y}(D(\bar{f}))$ (car les $D(f)$ sont une base de topologie de Y, et $\mathcal{O}_Y$ est le faisceau associé à $\mathcal{O}_{0,Y}$). On a $D(\bar{f}) = D(f) \cap Y$. Donc $\Gamma(X)_f \to \Gamma(Y)_{\bar{f}}$ est surjectif. Donc $R(D(\bar{f})) = \Gamma(Y)_{\bar{f}} \subset \mathcal{O}_{0,Y}(D(\bar{f}))$. Réciproquement, soit $\bar{s} \in \mathcal{O}_{0,Y}(D(\bar{f}))$. C'est la restriction de $s \in \mathcal{O}_X(U)$ ou U ouvert tel que $U \cap Y = D(\bar{f})$. Posons $U = \bigcup_{i\in I} D(g_i)$. Donc $D(\bar{f}) = \bigcup_{i\in I}(Y \cap D(g_i))$. De plus $s|_{D(g_i)} \in \mathcal{O}_X(D(g_i))$. Donc $\bar{s}|_{D(\bar{g}_i)} \in \Gamma(Y)_{\bar{g}_i} = R_Y(D(\bar{f}))$. □

Définition 2.13.10. Une sous-variété algébrique de X est $Z \subset X$ localement fermé (intersection d'un ouvert et d'un fermé), avec $\mathcal{O}_Z$ comme ci-dessus.

2.14 Aspects locaux

Soit X une variété algébrique. Soit $x \in X$. Considérons $\{(U, f) \mid U \text{ ouvert de } X,\ f \in \Gamma(U, \mathcal{O}_X)\}$. On le munit de la relation $\sim$ donnée par $(U, f) \sim (V, g)$ ssi il existe W ouvert de X avec $x \in W \subset U \cap V$ et $f|_W = g|_W$. C'est une relation d'équivalence. La classe de (V, f) s'appelle le germe de f en x. On pose $\mathcal{O}_{X,x} = \{germes\ de\ fonctions\ sur\ x\}$.

Proposition 2.14.1. *$\mathcal{O}_{X,x}$ est un anneau, et une $K-$algbre locale d'idéal maximal.*

$$\{germes\ de\ fonction\ f\ telle\ que\ f(x) = 0\} = m_{X,x}.$$

On a $\mathcal{O}_{X,x}/m_{X,x}$ est un corps isomorphe à K.

Démonstration. Soient $\bar{f}, \bar{g} \in \mathcal{O}_{X,x}$ de représentations f_1, g_1 et aussi f_2, g_2. On a $\overline{f_1 + g_1} = \overline{f_2 + g_2}$, $\overline{f_1 g_1} = \overline{f_2 g_2}$ sur $U_1 \cap U_2$ avec f_1, g_1 définies sur U_1 et f_2, g_2 définies sur U_2. D'où l'addition et multiplication sur $\mathcal{O}_{X,x}$. On vérifie qu'on a bien un anneau.

Soit $\bar{f} \in \mathcal{O}_{X,x}$ de représentant f. Alors $f(x) \in K$ est bien défini. L'application $\mathcal{O}_{X,x} \to K$ est surjective, de noyau un idéal maximal. C'est $m_{X,x}$. Si $f \notin m_{X,x}$, on a $f \in \mathcal{O}_{X,x}^{\times}$. En effet il existe un ouvert U au lequel f est défini et $x \in D(f) \cap U$ car $\bar{f} \in m_{X,x}$. Alors f est inversible, $\Gamma(D(f) \cap U, \mathcal{O}_x)$ et donc f inversible dans $\mathcal{O}_{X,x}$. □

Rappel : K est algébriquement clos.

Proposition 2.14.2. *Soit U un ouvert affine de X avec $x \in U$. Posons $A = \Gamma(U, \mathcal{O}_X)$ et $m = \{f \in A\ telle\ que\ f(x) = 0\}$. Alors on a un isomorphisme d'anneaux $\mathcal{O}_{X,x} \simeq A_m$ (localisé de A pour $A - m$).*

Démonstration. Considérons $A \to \mathcal{O}_{X,x}$ qui à f associe le germe de f dans $\mathcal{O}_{X,x}$. Si $f \notin m$, on a $\bar{f} \notin m_{X,x}$.

Donc $A \to A_{X,x}$ se factorise par $A \to A_m$. Considérons $A_m \to \mathcal{O}_{X,x}$. Elle est surjective. En effet, soit g de germe $\bar{g} \in \mathcal{O}_{X,x}$ avec g défini sur $D(f)$. On a $D(f) \cap U \subset U$. On a

$$\begin{array}{ccccc} \Gamma(U, \mathcal{O}_X) & \longrightarrow & \Gamma(D(f) \cap U, \mathcal{O}_X) & \longrightarrow & \mathcal{O}_{X,x} \\ \| \uparrow & & \| \uparrow & & \uparrow \\ A & \longrightarrow & \Gamma(U, \mathcal{O}_X)_f & \longrightarrow & A_m \end{array}$$

Donc $g = \frac{u}{f}$ provient de $\Gamma(U, \mathcal{O}_X)_f$. D'où la surjectivité. Vérifions l'injectivité. Soit $\frac{a}{b} \in A_m$, i.e. $a \in A$, $b \in A \backslash m$ tel que le germe de $\frac{a}{b}$ soit 0 dans $\mathcal{O}_{X,x}$. Donc $\frac{a}{b} = 0$ dans A_f et on a un morphisme $A_f \to A_m$ donc $\frac{a}{b} = 0$ dans A_m. □

Le dictionnaire qui permet de passe des idéaux premiers d'une $K-$algèbre réduite aux fermés irréductibles d'une variété algébrique affine donne la correspondance :

$$\{\textit{idéaux premiers } \mathcal{O}_{X,x}\} \longleftrightarrow \left\{ \begin{array}{c} \textit{fermés irreductible de } U \\ \textit{contenant } x \textit{ (et donc de } X) \end{array} \right\}.$$

Soit $\varphi : X \to Y$ un morphisme de variétés algébriques. Soit $x \in X$. Posons $y = \varphi(x)$. On a alors $\varphi^* : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ donné aussi. Soit $\bar{f}$ germe de (U, f) avec U ouvert de Y, $y \in U$. On considère

$$\begin{array}{c} \varphi^* : \Gamma(U, \mathcal{O}_Y) \longrightarrow \Gamma(\varphi^{-1}(U), \mathcal{O}_X) \\ f \longmapsto f \circ \varphi. \end{array}$$

L'image $\varphi^*(\bar{f})$ est le germe de $(\varphi^{-1}(U), f \circ \varphi)$. On a $m_{Y,y} \subset \varphi^*(m_{X,x})$. Si φ est un isomorphisme, φ^* est un isomorphisme.

La catégorie des variétés algébriques pointées a pour objets les (X, x) où X est une variété algébrique et $x \in X$. Les morphismes $(X, x) \to (Y, y)$ sont les morphismes $\varphi : X \to Y$ de variétés algébriques tels que $\varphi(x) = y$. La catégorie des anneaux locaux a pour objets les anneaux locaux et pour morphismes $A \to B$ les morphismes d'anneaux $f : A \to B$ tels que $f(\textit{idéal maximal de } A) \subset \textit{idéal maximal de } B$.

$(X, x) \to \mathcal{O}_{X,x}$ est un foncteur contravariant de la catégorie des variétés algébriques pointés vers la catégorie des anneaux locaux.

2.15 Variétés algébriques projectives

Soit V un ensemble algébrique projetif $\subset \mathbb{P}^m$. Il est muni de la topologie de Zariski. On veut en faire une variété algébrique. Pour cela il fait défini uu faisceau d'anneaux. Pour cela définissons ce faisceau sur une base d'ouverts de V : pose $f \in \Gamma_h(V) = K[X_0, \cdots, X_n]/I(V)$, les $D^+(f) = \{(x_0, \cdots, x_n) \in V \mid f(x_0, \cdots, x_n) \neq 0\}$ avec $d^\circ f > 0$ constituent une base d'ouverts

de V.

Pour $f = X_0$, on a $D^+(X_0) = \{(x_0, \cdots, x_n) \in \mathbb{P}^n,\ x_0 \neq 0\}$. On a $j : K^n \simeq D^+(X_0) = U_0$. Les fonctions sur U_0 correspondant aux polynômes en $\frac{X_1}{X_0}, \cdots, \frac{X_n}{X_0}$. On pose $\Gamma(U_0, \mathcal{O}_{\mathbb{P}^n}) = K\left[\frac{X_1}{X_0}, \cdots, \frac{X_n}{X_0}\right]$.

Soit A un anneau gradué. Soit $f \in A$ homogène de degré d. On munit A_f (localisé de A par $\{f^n,\ n \geq 0\}$) d'une graduation en posant (faux ?)

$$A_{e-rd} = \{\frac{g}{f^r} \mid g \in A \textit{ homogne de degré } e\}.$$

On a $A_{(f)} = \{P \in A_f \mid d^\circ P = 0\}$. Pour $P \in A_{(f)}$, $P(x_0, \cdots, x_n)$ bien défini pour les coordonnées homogènes $(x_0, \cdots, x_n)$. D'où des fonctions sur $D^+(f)$. On pose pour $f \in \Gamma_h(V)$ homogène de dégré> 0, $\Gamma(D^+(f), \mathcal{O}_V) \simeq \Gamma_h(V)_{(f)}$. D'où un faisceau $\mathcal{O}_V$ d'anneaux sur V.

Proposition 2.15.1. *Cela fait de $(V, \mathcal{O}_V)$ une variété algébrique.*

Démonstration. Soit $\overline{F} \in \Gamma_h(V)$ classe de $F \in K[X_0, \cdots, X_n]$. On a $D^+(\overline{F}) = V \cap D^+(F)$. On considère

$$\begin{array}{ccc} r : \Gamma(D^+(F), \mathcal{O}_{\mathbb{P}^n}) & \longrightarrow & \Gamma(D^+(F), \mathcal{O}_V) \\ \| & & \| \\ K[X_0, \cdots, X_n]_{(F)} & \longrightarrow & \Gamma_h(V)_{(\overline{F})}. \end{array}$$

qui est surjective.

Donc pour montrer que V est une variété algébrique, il suffit de montrer que $\mathbb{P}^n$ est une variété algébrique.

L'espace $\mathbb{P}^n$ recouvert par les $D^+(X_i)$. Pour $0 \leq i \leq n$, il suffit de montrer que $D^+(X_i)$ est une variété algébrique.

Faisons le pour $i = 0$. Posons $U_0 = D^+(X_0)$,

$$\begin{aligned} j : K^n &\longrightarrow U_0 \\ (x_1, \cdots, x_n) &\longmapsto (1, x_1, \cdots, x_n). \end{aligned}$$

Vérifions que c'est un homéomorphisme et un isomorphisme d'espace annelés. Montrons que j et j^{-1} sont continues, i.e.

$$j(\textit{ouvert standard}) \textit{ estunouvert},\ j^{-1}(\textit{ouvert standard}) \textit{ estunouvert}.$$

Soit $F \in K[X_0, \cdots, X_n]$ homogène. On a $j^{-1}(D^+(F)) = j(D^{-1}(F) \cap U_i) = D(f)$ où $f\left(\frac{X_1}{X_0}, \cdots, \frac{X_n}{X_0}\right) = \frac{F(X_0, \cdots, X_n)}{X_0^{d^\circ F}}$. De même pour $f \in K[X_0, \cdots, X_n]$, on a $j(D(f)) = D^+(F) \cap U_0$ où $F(X_0, \cdots, X_n) = X_0^d \underbrace{f\left(\frac{X_1}{X_0}, \cdots, \frac{X_n}{X_0}\right)}_{K[X_0, \cdots, X_n]}$ où $f = f_0 + f_1 + \cdots + f_d$ avec f_i homogène de degré i. Donc $j(D(f))$ est ouvert.

Donc, j est un homéomorphisme. Il reste à montrer que $\Gamma(D^+(F) \cap U_0, \mathcal{O}_{\mathbb{P}^n}) \simeq \Gamma(D(f), \mathcal{O}_{K^n})$, on a $D^+(F) \cap U_0 = D^+(X_0 F)$. Donc $\Gamma(D^+(F) \cap U_0, \mathcal{O}_{\mathbb{P}^n}) \simeq K[X_0, \cdots, X_n]_{(X_0 F)} = \{\frac{f}{(FX_0)^r}\ avec\ d^\circ P = r(d^\circ F + 1)\}$. Par ailleurs, $\Gamma(D(f), \mathcal{O}_{K^n}) = K[X_1, \cdots, X_n]_f$. On obtient l'isomorphisme ainsi.

$$K[X_0, \cdots, X_n]_{(FX_0)} \longrightarrow K[X_0, \cdots, X_n]_{FX_0} \longrightarrow K[X_0, \cdots, X_n]_f$$

$$\frac{P}{F^r X_0^s} \longmapsto \frac{P(X_0, \cdots, X_n)}{F(X_0, \cdots, X_n)^r} \cdot X_0^n$$

avec $n = rd^\circ F - d^\circ f$. C'est un morphisme de $K-$algèbre. C'est injectif, car si $P\left(\frac{X_1}{X_0}, \cdots, \frac{X_n}{X_0}\right) = 0$, on a $P = 0$. C'est surjectif car $\frac{g}{f^r} \in K[X_0, \cdots, X_n]_f$ a pour image réciproque $\frac{G}{F^r X_0^s}$ où $s = rd^\circ f - d^\circ g$ et $G(X_0, \cdots, X_n) = X_0^d g\left(\frac{X_1}{X_0}, \cdots, \frac{X_n}{X_0}\right)$. Donc U_0 est une variété algébrique, et alors $\mathbb{P}^n$ et V le sont.

Une variété algébrique projective est une variété algébrique isomorphe à un ensemble algébrique projectif muni de ce faisceau.

Les variétés algébriques projectives forment une catégorie dont les morphismes sont les mor-

phismes de variétés algébriques.

Exemple de fermé F dans une variété algébrique X pour lequel $(F, \mathcal{O}_{X|F})$ n'est pas au faisceau. On considère $X = \mathbb{P}^2$, $F = V(I)$ où I idéal homogène de $K[X, Y, Z]$ engendré par $\{X(X - Z),\ XY\}$.

Si X est une variété algébrique projective irréductible, on a $\Gamma(X, \mathcal{O}_X) = K$ (composer au théorème de Liouville à toute fonction holomorphe bornée sur $\mathbb{C}$ est constante).

$$\begin{array}{ccc} \textit{variétés algébrique} & \longleftrightarrow & \begin{array}{c} K - \textit{algèbre réduites} \\ \textit{de type fini} \end{array} \\ \cap & & \cap \\ \textit{schéma} & \longleftrightarrow & \textit{Anneau commutatif.} \end{array}$$

Alexandre Grothendieck (1928-2014). □

Chapitre 3

Algèbre Homologique

3.1 Complexes

Soit A un anneau. Notons $\mathcal{M}od(A)$ la catégorie des $A-$modules. Un complexe de $A-$modules est constitué de A modules E', pour $i \in \mathbb{Z}$ et de morphismes $d^i : E \to E^{i+1}$ avec $d^i \circ d^{i+1} = 0$, $(\operatorname{Im} d^{i-1} \subset \ker d^i)$. On la représente aussi :

$$\cdots E^{i-1} \xrightarrow{d^{i-1}} E^i \xrightarrow{d^i} E^{i+1} \longrightarrow \cdots$$

On peut le noter (E, d). d_i s'appelle le bord ou la différentielle.

Notation duale, on note E_i plutôt que E^i et $d_i : E_i \to E_{i-1}$. On a $d_{i-1} \circ d_i = 0$. On représente le complexe ainsi

$$\cdots E^{i-1} \xrightarrow{d^{i-1}} E^i \xrightarrow{d^i} E^{i+1} \longrightarrow \cdots$$

Si $\{i \mid E^i \neq 0\}$ est fini, on dit que le complexe est fini ou borné.

On dit que (E, d) est exact si $\operatorname{Im} d^{i-1} = \ker d^i$ pour tout $i \in \mathbb{Z}$. On dit que le complexe est une suite exacte. Les complexes, exactes de la forme

$$0 \longrightarrow E' \longrightarrow E \longrightarrow E'' \longrightarrow 0$$

sont dits suites exactes courtes. Alors E' est isomorphe à un sous-module F de E et E'' est isomorphe à E''/F.

Soit (E, d) un complexe. On pose $H_i(E) = \ker d^i / \operatorname{Im} d^{i-1}$. (E, d) est exact ssi $H_i(E) = \{0\}$ pour tout i. $H_i(E)$ est le i-ème module d'homologie du complexe. Il mesure le défaut d'exactitude du complexe.

Soit M un $A-$module. Un complexe exact de la forme

$$\cdots \longrightarrow E_1 \longrightarrow E_0 \longrightarrow M \longrightarrow 0$$

s'appelle une résolution de M.

–On dit que la résolution est libre si E_i est un $A-$module libre pour tout $i \geq 0$.

–On dit que la résolution est finie si on a $E_i = 0$ ($0 = \{0\}$ par convention) pour i assez grand.

Proposition 3.1.1. *Tout $A-$module admet une résolution libre.*

Démonstration. Soit M un $A-$module. Soit S une partie génératrice de M. On peut considérer $A[S]$ le $A-$module libre engendré par S. On a un morphisme de $A-$module

$$\begin{aligned} A[S] &\longrightarrow M \\ \sum_s \lambda_s [s] &\longmapsto \lambda_s s. \end{aligned}$$

Il est surjectif, car S partie génératrice. Donc on a

$$\underbrace{A[S]}_{=E_0} \longrightarrow M \longrightarrow 0.$$

Notons N_1 le noyau. C'est un $A-$module. C'est un quotient d'un $A-$module libre E_1, on a donc

$$E_1 \longrightarrow E_0 \longrightarrow M \longrightarrow 0.$$

Notons N_2 le noyau de $E_1 \longrightarrow E_0$. C'est un quotient de E_2, $A-$module libre etc. On obtient la résolution libre. □

Si M admet une résolution finie

$$\cdots \longrightarrow E_0 \longrightarrow M \longrightarrow 0$$

$\max\{i \mid E_i \neq 0\}$ s'appelle la longueur de la résolution.

Soit S un ensemble fini. On pose $E_i = \mathbb{Z}[S^{i+1}]$. C'est un $\mathbb{Z}-$module. On pose $d_i : E_i \to E_{i-1}$, $d_i(x_0, \cdots, x_i) = \sum_{j=0}^{i}(-1)^j(x_0, \cdots, \widetilde{x_j}, \cdots, x_i)$ où $(x_0, \cdots, \widetilde{x_j}, \cdots, x_i) = (x_0, \cdots, x_{j-1}, x_{j+1}, \cdots, x_i)$. On a $E_0 = \mathbb{Z}[S]$. On pose $d_0 : E_0 \to \mathbb{Z}$ tel que $d([x_i]) = 1$. On obtient une résolution de $\mathbb{Z}$.

$$\cdots \longrightarrow E_1 \xrightarrow{d_1} E_0 \xrightarrow{d_0} \mathbb{Z} \longrightarrow 0.$$

C'est le complexe standard. Soit M un $A-$module est un complexe (E, d). Comme $d^{i-1} : E^{i-1} \to E$, on pose

$$\begin{aligned} S^i : Hom_A(E^i, M) &\longrightarrow Hom(E^{i-1}, M) \\ f &\longmapsto f \circ d^{i-1}. \end{aligned}$$

On obtient un complexe"

$$\cdots \longrightarrow Hom(E^{i+1}, M) \longrightarrow Hom(E^i, M) \longrightarrow Hom(E^{i-1}, M) \longrightarrow \cdots$$

Soient (E, d) et (E', d') des complexes. Un morphisme de complexe de degré$\geq r$ $(E, d), (E', d')$ est la donnée de morphismes de $A-$modules $f_i : E^i \to E^{i+r}$ pour $i \in \mathbb{Z}$ tels que les diagrammes

$$\begin{array}{ccc} E^{i-1} & \xrightarrow{f} & E'^{i-1+r} \\ \downarrow{\scriptstyle d^{i-1}} & & \downarrow{\scriptstyle d'^{i-1+r}} \\ E^i & \xrightarrow{f} & E'^{i+r} \end{array}$$

commutent. C'est-à-dire $d^{i-1+r} \circ f_{i-1} = f_i \circ d^{i-1}$. Ainsi les complexes de $A-$modules forment une catégories dont les morphismes sont les morphismes de complexes de tout degré.

Soit $f : (E, d) \to (E', d)$ un morphisme de complexes. On peut considérer $(\ker f_i)_{i\in\mathbb{Z}} = \ker f$ et $(\operatorname{Im} f_i)_{i\in\mathbb{Z}} = \operatorname{Im} f$. Alors $(\ker f, d)$ et $(\operatorname{Im} f, d')$ sont des complexes.

Rappel : pour tout $i \in \mathbb{Z}$, $\operatorname{coker}(f_i) = E'^{i+1}/\operatorname{Im}(f_i)$ et $\operatorname{Coim}(f_i) = E_i/\ker(f_i)$.

Alors $(\operatorname{coker}, d^i)$ et (Coim, d) sont des complexes.

Si pour tout i, F^i est un sous-$A-$module de E^i et que $i : F \to E$ est un morphisme de complexes (de degré 0), on dit que (F, d) est un sous-complexe de (E, d). Alors on a un complexe quotient $(E/F, d)$

$$\cdots \longrightarrow E^{i-1}/F^{i-1} \longrightarrow E^i/F^i \longrightarrow E^{i+1}/F^{i+1} \longrightarrow \cdots$$

On peut considérer les sommes directes et des produits de complexes.

On a vu la notion d'anneau gradué et de module gradué. Soit (E, d) un complexe de $A-$module. Posons $M = \bigoplus^{i\in\mathbb{Z}} E^i$. L'anneau A a pour seule graduation $A = A_0$ (à priori).

On considérons l'anneau gradué $A[X] = \bigoplus_{i>0} AX^i$. Alors M est un $A[X]-$module en posent $X \cdot (\sum_{i\in\mathbb{Z}} m_i) = \sum_{i\in\mathbb{Z}} d^i(m_i)$ (avec $m_i \in E^i$). On a $X^2 \cdot m = 0$ pour tout $m \in M$. (En fait, M est un $A[X]/(X^2)-$module) De plus, M est un $A[X]-$module gradué.

Comme $X^2 \cdot m = 0$, on dit que M est un $A-$module différentiel gradué. Comme $d(E_i) \subset E_{i-1}$, on dit que la différentielle est de degré 1. Comme $d(E^i) \subset E^{i+1}$, on dit que la différentielle est de degré -1.

On dit qu'un complexe est formé de longueur n si E^i, d^i ne dépendent que de la classe de i dans $\mathbb{Z}/n\mathbb{Z}$.

$$E^0 \longrightarrow E^1 \longrightarrow \cdots \longrightarrow E^n$$

3.2 Au-delà des modules sur les anneaux commutatifs

Soit A un anneau (non nécessairement commutatif). Un $A-$module à gauche est un groupe abélien M muni d'une loi

$$\begin{aligned} A \times M &\longrightarrow M \\ (a, m) &\longmapsto am \end{aligned}$$

qui vérifie

$$\begin{cases} 1 \cdot m = m \\ a \cdot (m + m') = am + am' \\ (a + a')m = am + a'm \\ (aa') \cdot m = a \cdot (a' \cdot m). \end{cases}$$

Pour tous $m, m' \in M$, $a, a' \in A$. (Si, au lieu de $(aa') \cdot M = a \cdot (a' \cdot m)$ on a $(aa') \cdot M = a' \cdot (a \cdot m)$, on dit que M est un $A-$module à droite).

On a des notions de sous-module, de quotient, de noyau, d'image, de conoyau, de coimage, de complexe et d'exactitude.

La théorie des complexes s'étend aux modules sur des anneaux noncommutatifs.

En particulier, si $E.$ est un groupe et B un anneau commutatif. On a la $B-$algèbre $B[G]$ où la multiplication est donnée par

$$\begin{aligned} B[G] \times B[G] &\longrightarrow B[G] \\ (\sum_{g \in G} b_g [g]) \cdot (\sum_{g \in G} b'_g [g]) &\longmapsto \sum_{h \in G} \sum_{g \in G} b_g b'_{g^{-1}h} [h]. \end{aligned}$$

$B[G]$ est un anneau commutatif ssi G est commutatif.

On peut considérer les $B[G]-$modules à gauche.

Si $B = \mathbb{C}$, les $\mathbb{C}[G]-$modules à gauche sont exactement les représentations complexes du

groupe G.

Si $B = \mathbb{Z}$, on parle de $G-$module à gauche. Soit $(X, \mathcal{O}_X)$ un espace annelé. Un $\mathcal{O}_X-$module est un faisceau $\mathcal{F}$ sur X tel que pour tout ouvert U de X, $\mathcal{F}(U)$ est un $\mathcal{O}_X(U)-$module avec pour tout V ouvert, $V \subset U$ on a $r^{\mathcal{F}}_{V,U} : \mathcal{F}(U) \to \mathcal{F}(V)$ est linéaire. C'est-à-dire

$$r^{\mathcal{F}}_{V,U}(af + bg) = r^{\mathcal{F}}_{V,U}(a) r^{\mathcal{F}}_{V,U}(f) + r^{\mathcal{F}}_{V,U}(b) r^{\mathcal{F}}_{V,U}(g)$$

pour $a, b \in \mathcal{O}_X(U),\ f, g \in \mathcal{F}(U)$.

Soient $\mathcal{F}$ et $\mathscr{G}$ des $\mathcal{O}_X-$modules sur X. Un morphisme de $\mathcal{O}_X-$modules est la donnée, pour tout ouvert U de X, d'un morphismes de $\mathcal{O}_X-$modules $f_U : \mathcal{F}(U) \to \mathscr{G}(U)$ compatible aux restrictions, i.e. le diagramme

commute.

Le noyau d'un tel morphisme est le faisceau $\ker(f)$ tel que $\ker(f)(U) = \ker(f_U)$. C'est un faisceau de $\mathcal{O}_X-$modules.

On peut considérer pour tout U ouvert de X. $\mathrm{Im}(f)(U) = \mathrm{Im}(f_U)$. Mais on n'a pas un faisceau en général. C'est un préfaisceau. Il faut considérer le faisceau associé. On pose

$$\mathrm{Im}(f)(U) = \left\{ s \in \mathscr{G}(U) \;\middle|\; \begin{array}{c} \textit{pour tout } x \in U \textit{ il existe } V \textit{ ouvert,} \\ x \in V \subset U \textit{ et } s|_U = \mathrm{Im}(f_V) \end{array} \right\}.$$

Ainsi on obtient le faisceau image de f, noté $\mathrm{Im}(f)$. On dit que f est surjectif si $rmIm(f) = \mathscr{G}$. Alors on a les notions de noyau, image, quotient, somme, produit, suite exacte, complexe homologie.

3.3 Homologie

Revenons aux modules sur les anneaux commutatif. Soit A un anneau. Soit (E, d) un complexe de $A-$modules. On note

$$Z^i(E) = \ker d^i \ (ensembledesi - cycles)$$

$$B^i(E) = \operatorname{Im} d^{i+1} \ (ensembledesi - bords)$$

On pose

$$H^i(E) = Z^i/B^i \ i - memoduled'homologie$$

(plutôt $H_i(E)$, car H^i désigne la cohomologie) Soit $f : (E', d') \to (E, d)$ un morphisme de degré 0. On peut le voir comme un morphisme deifférentielles gradués. Pour tout $i \in \mathbb{Z}$, il donne lieu à $H_i(f)$ ou $f_i : H'_i(E') \to H_i(E)$ (bien défini). On pose $H(E') = \bigoplus_{i\in\mathbb{Z}} H_i(E')$ et $H(E) = \bigoplus_{i\in\mathbb{Z}} H_i(E)$.

Ce sont des modules gradués. Donc H est un foncteur de la catégorie des complexes vers la catégorie des modules graduées.

Un complexe de complexes est au complexe de $A-$modules différentiels gradués.

Soit $0 \to E' \to E \to E'' \to 0$ une suite exacte courte de complexes. Elle s'écrit

$$\begin{array}{ccccccccc}
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E'^{i-1} & \xrightarrow{f_{i-1}} & E^{i-1} & \xrightarrow{g_{i-1}} & E''^{i-1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'^{i-1}} & & \downarrow{\scriptstyle d^{i-1}} & & \downarrow{\scriptstyle d''^{i-1}} & & \\
0 & \longrightarrow & E'^{i} & \xrightarrow{f_{i}} & E^{i} & \xrightarrow{g_{i}} & E''^{i} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'^{i}} & & \downarrow{\scriptstyle d^{i}} & & \downarrow{\scriptstyle d''^{i}} & & \\
0 & \longrightarrow & E'^{i+1} & \xrightarrow{f_{i+1}} & E^{i+1} & \xrightarrow{g_{i+1}} & E''^{i+1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & &
\end{array}$$

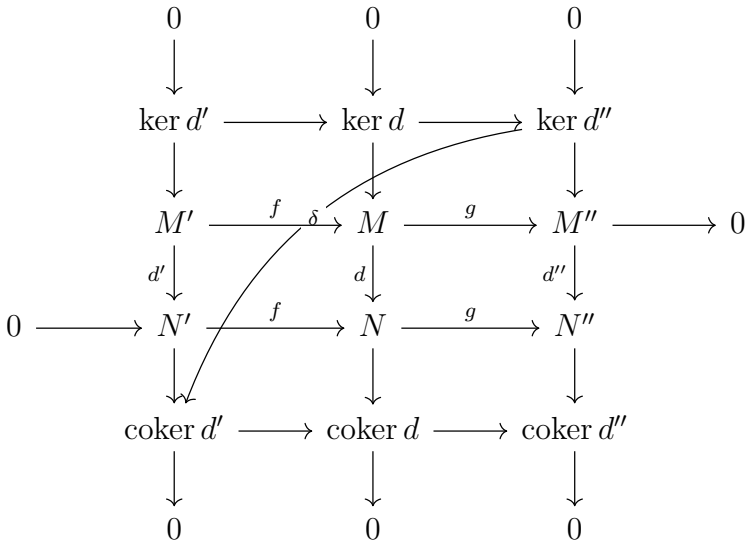
Proposition 3.3.1. *(lemme du serpent) Soient des morphismes de $A-$modules*

$$\begin{array}{ccccccccc}
 & & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\
 & & {\scriptstyle d'}\downarrow & & {\scriptstyle d}\downarrow & & {\scriptstyle d''}\downarrow & & \\
0 & \longrightarrow & N' & \xrightarrow{\tilde{f}} & N & \xrightarrow{\tilde{g}} & N'' & &
\end{array}$$

dont les lignes sont des complexes exactes, qui commute (les colonnes sont des complexes exacts par définition). On a $\delta = \ker(d'') \to \operatorname{coker}(d')$ tel qu'on ait une suite exacte.

$$\ker(d') \to \ker(d) \to \ker(d'') \xrightarrow{\delta} \operatorname{coker}(d') \to \operatorname{coker}(d) \to \operatorname{coker}(d'')$$

Démonstration.



Idée : $s(z'') = f^{-1} \circ d \circ g^{-1}(z'')$. Soit $z'' \in \ker d$. Il existe $z \in M$ tel que $g(z) = z''$ (bien défini à $f(M')$ près). On a $d(z) \in N$ et $gd(z) = d''g(z) = d''(z'') = 0$. Donc $d(z) \in \ker g$ et il existe $w' \in N'$ tel que $f(w') = d(z)$. Soit $\delta(v'') =$image de w' dans $\operatorname{coker} d'$.

Si on fait un autre choix pour z, disons z_0, on a $z - z_0 \in f(M')$ et

$$\begin{aligned} d(z_0) &= d(z_0 - z) + d(z) \\ &\overset{z_0 - z \in f(M')}{=\!=\!=} d(z) + df(y') \\ &= d(z) + fd'(y'). \end{aligned}$$

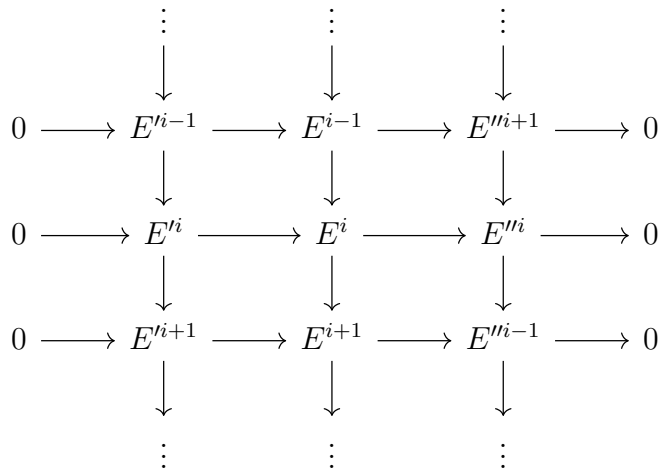
Donc $f^{-1}(d(z_0)) = f^{-1}(d(z)) + d'(y)$, dont les images sont coïncide dans $\operatorname{coker} d'$.

Vérifions l'exactitude de la suite. Soit $z'' \in \ker \delta$, montrons que $z'' \in g(\ker d)$. On a $w' \in d'(M')$. Donc $f(w') \in f \circ d'(M') = d \circ f(M') = d(\ker g)$. Donc $d(z) \in d(\ker g)$ et alors $z \in \ker g + \ker d$. Donc $g(z) \in \ker d''$. □

Théorème 3.3.2. *Soit $0 \to E' \xrightarrow{f} E \xrightarrow{g} E'' \to 0$ une suite exacte de complexes avec f, g de degré 0. Alors on a une suite exacte de modules gradués*

On a un foncteur de la catégorié des suites exactes courtes vers la catégorie des complexes.

Démonstration. On a



Du lemme du serpent, on déduit

$$\delta^i : H^i(E'') \to H^{i+1}(E')$$

δ est un morphisme de complexes de degré 1. On a donc une suite exacte

$$\to H^i(E') \xrightarrow{f_*} H^i(E) \xrightarrow{g_*} H'(E'') \xrightarrow{\delta} H^{i+1}(E') \to$$

□

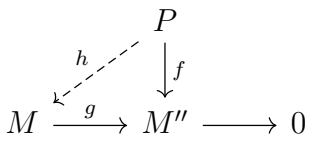
3.4 Modules projectifs

Soit A un anneau. Soit P un $A-$module. On dit que la foncteur $Hom_A(P, \cdot)$ est exact si pour toute suite exacte de $A-$modules $0 \to M' \to M \to M'' \to 0$. On déduit

$$0 \to Hom_A(P, M') \to Hom_A(P, M) \to Hom_A(P, M'') \to 0$$

(C'est à dire que $Hom_A(P, M) \to Hom_A(P, M'')$ est surjectif). On dit que P est un module projectif si pour tout morphisme de $A-$module $P \xrightarrow{f} M''$ et touts morphismes $g : M \to M''$

surjectif, il existe $h : P \to M$ morphisme t.q. $f = g \circ h$



Proposition 3.4.1. *Les conditions suivants sont équivalentes :*

1. *$Hom_A(P, \cdot)$ est exact ;*
2. *P est un module projectif ;*
3. *Toute suite exacte $0 \to M' \to M \to P \to 0$ est scindée ;*
4. *Il existe un $A-$module libre L et une $A-$module P' tels que L est isomorphe à $P \times P'$.*

Remarques 3.4.2. *Sur 3., une suite exacte courte $0 \to M' \xrightarrow{i} M \to M'' \to 0$ est dite scindée si la surjection $M \to M''$ admet une section s qui est un morphisme et dont l'image est un supplémentaire de l'image de M' dans M. On a $M = s(M'') \oplus i(M')$.*
Sur 4., on dit alors que P est un facteur direct de L.

Démonstration. 1⇒ 2 : On a $f : P \to M''$ et $g : M \to M''$ surjectif. On considère la suite exacte $0 \to \ker g \to M \to M'' \to 0$. Donc la suite exacte $0 \to Hom(P, \ker g) \to Hom(P, M) \to Hom(P, M'') \to 0$. Donc il existe $h : P \to M$ tel que $f = g \circ h$.

2⇒3 : Soit $0 \to M' \to M \xrightarrow{g} P \to 0$ une suite exacte. On applique 2. à $M'' = P$ et $f = id$. Il existe $h : P \to M$ tel que $id = g \circ h$. Donc h est la section cherchée.

3⇒4 : Ecrivons P comme quotient d'un module libre L. On a une suite exacte $0 \to P' \to L \to P \to 0$. Comme cette suite exacte est scindée, on a L isomorphe à $P' \times P'$.

4⇒1 : Posons $L = P \oplus P'$. Montrons que P est projectif. Posons $L = A^{(S)}$ (module libre base S). Alors $Hom_A(L, M) = Hom_A(A^{(S)}, M) = M^{(S)}$. Donc $Hom_A(L, \cdot)^A$ est exact ssi $M^{(S)} \to M''^{(S)}$ est surjectif des lors que $M \to M''$ est surjective. C'est évident comme $L \simeq P \times P'$, on a $Hom_A(L, \cdot) \simeq Hom_A(P, \cdot) \times Hom_A(P', \cdot)$. Donc $Hom_A(P, \cdot)$ est exact. □

Corollaire 3.4.3. *Tout module libre est projectif. Tout module est quotient d'un module projectif.*

Remarques 3.4.4.

1. *La notion de projectif a un sens au delà des modules, dans d'entres catégories. (remplacer injectif/surjectif par monomorphisme/épimorphisme)*

2. *On a $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Le facteur direct $\mathbb{Z}/2\mathbb{Z}$ est un $\mathbb{Z}/6\mathbb{Z}-$module projectif. (car facteur direct de $\mathbb{Z}/6\mathbb{Z}$, qui est libre. Mais il n'est pas libre.)*
3. *Lorsque A est de Dedekind, un idéal non principal I est un module projectif non libre.*

3.5 Modules injectifs

Soit Q un $A-$module. On dit que la foncteur $Hom_A(\cdot, Q)$ est exact si pour toute suite exacte courte $0 \to M' \to M \to M'' \to 0$, on déduit une suite exacte $0 \to Hom_A(M'', Q) \to Hom_A(M, Q) \to Hom_A(M'', Q) \to 0$. On dit que Q est un module injectif si pour tout morphisme $i : M \to M'$ injectif et tout $f : M \to Q$. Il existe $g : M' \to Q$ tel que $f = g \circ i$.

Notion duale de "projectif" qui s'applique à autres catégories que les catégories de modules. (Il faut imposer qui i est un monomorphisme).

Proposition 3.5.1. *Les assertions suivantes sont équivalentes :*

1. *Q est injectif ;*
2. *$Hom_A(\cdot, Q)$ est exacte ;*
3. *Toute suite exacte $0 \to Q \to M \to M'' \to 0$ est scindée.*

Démonstration. 1.⇔2. : immédiat.
(1. ou 2.)⇒3. : on applique au diagramme

il existe $h : Q \to M$ tel que $h \circ i = id$. Donc $\ker h$ est le supplémentaire de $i(Q)$.

3.⇒(1. ou 2.) : considérons

Posons $Q' = Q \oplus_{M'} M = {Q \times M}\Big/{\{(q, m) \in Q \times M \mid il existe m' \in M' avec \alpha(m') = m, \beta(m') = -q\}}$.
Alors $M' \to Q'$ est injective et on a

$$0 \to Q \to Q' \to {Q'}/{\operatorname{Im} Q} \to 0$$

exacte donc scindée. Donc $Q' = \operatorname{Im} Q \oplus Q''$ et on a $Q' \to Q$. D'où $M \to Q' \to Q$ convient pour prolonger β à M. □

Soit H un groupe abélien. Considérons

$$\begin{aligned}\mathbb{Q}/\mathbb{Z} &\xrightarrow{\sim} \{z \in \mathbb{C}^\times,\ racine\ de\ l'unit\}\\ k+z &\longmapsto e^{2i\pi k}.\end{aligned}$$

Le groupe $Hom_{\mathbb{Z}}(H, \mathbb{Q}/\mathbb{Z})$ s'appelle le dual de Pontrjagin de H. On le note $\widehat{H}$. Si H est un $A-$module, $\widehat{H}$ est un $A-$module par

$$\begin{aligned}A \times \widehat{H} &\longrightarrow \widehat{H}\\ (a, \varphi) &\longmapsto (h \longmapsto \varphi(ah)).\end{aligned}$$

On dit que H est divisible si pour tout $n \in \mathbb{Z}$, $n \neq 0$, l'application $H \overset{\times n}{\to} H$ est surjective.

Proposition 3.5.2. *Si H est divisible, c'est un $\mathbb{Z}-$module injectif.*

Démonstration. Soit $G' \to G$ un morphisme injectif de $\mathbb{Z}-$modules. On identifie G' à un sous-groupe de G. Soit $f : G' \to H$ un morphisme de $\mathbb{Z}-$modules. On veut prolonger f de G' à G. Considérons

$$\mathscr{E} = \left\{ (K, g) \;\middle|\; \begin{array}{c} K\ sous-groupe\ de\ G\ contenant\ G' \\ et\ g : K \to H\ qui\ prolonge\ f \end{array} \right\}.$$

On a une relation de bon ordre sur $\mathscr{E}$ donnée par $(K, g) \leq (K'g')$ ssi $K \subset K'$ et g' prolonge g. Soit (K_0, g_0) un élément maximal de $\mathscr{E}$. Soit $x \in G$. On veut étendre g_0 de K_0 à $K_0 + \mathbb{Z}x$. Si x est d'ordre infini dans G/K_0, on pose $g(x) = t$ où t est un élément quelconque de H. Si x est d'ordre fini n dans G/K_0, il existe $u \in H$ tel que $nu = g_0(nx)$ (car H divisible). On pose $g(z + nx) = g_0(z) + nu$. Donc $g : K_0 + \mathbb{Z}x \to H$ bien définit. Comme (K_0, g_0) est maximal, $K_0 + \mathbb{Z}x \subset K_0$. Donc $x \in K_0$. Donc $K_0 = G$, on a trouvé le prolongement. □

Exemples 3.5.3.

1. $\mathbb{Q}$, $\mathbb{Q}/\mathbb{Z}$, $\mathbb{R}$, $\mathbb{R}/\mathbb{Z}$ sont des $\mathbb{Z} - modules$ divisibles et donc injectifs.
2. Si L est un $\mathbb{Z}-$module libre, posons $L = \mathbb{Z}^{(S)}$, alors $\widehat{L} = Hom(\mathbb{Z}^{(S)}, \mathbb{Q}/\mathbb{Z}) = (\mathbb{Q}/\mathbb{Z})^S$ qui est divisible car $\mathbb{Q}/\mathbb{Z}$ est divisible. Donc $\widehat{L}$ est injectif.

Si M est un $A-$module et H est un $\mathbb{Z}-$module, $Hom_{\mathbb{Z}}(M, H)$ est un $A-$module.

Lemme 3.5.4. *On a des isomorphisme de $A-$modules*

$$\begin{aligned} Hom_{\mathbb{Z}}(M,H) &\xrightarrow{\sim} Hom_A(M, Hom_{\mathbb{Z}}(A,H)) \\ \psi &\longmapsto \big(m \mapsto (a \mapsto \psi(am))\big). \end{aligned}$$

(l'inverse est $f \mapsto (x \mapsto f(x)(1))$.)

Démonstration. Vérification immédiate. □

Lemme 3.5.5. *Si H est un $\mathbb{Z}-$module divisible, $Hom_{\mathbb{Z}}(A,H)$ est un $A-$module injectif.*

Démonstration. Soit $M \to M'$ un morphisme injectif de $A-$modules. Il faut montrer la surjectivité de

$$\begin{array}{ccc} Hom_A(M', Hom_{\mathbb{Z}}(A,H)) & \longrightarrow & Hom_A(M, Hom_{\mathbb{Z}}(A,H)) \\ \downarrow & & \downarrow \\ Hom_{\mathbb{Z}}(M',H) & \longrightarrow & Hom_{\mathbb{Z}}(M,H) \end{array}$$

□

Lemme 3.5.6. *Tout $A-$module est un sous-module d'un $A-$module divisible.*

Démonstration. Soit M un $A-$module, considérons $\widehat{\widehat{M}} = Hom_{\mathbb{Z}}(\widehat{M}, \mathbb{Q}/\mathbb{Z})$. On a un morphisme injectif de $A-$modules

$$\begin{aligned} M &\longrightarrow \widehat{\widehat{M}} \\ m &\longmapsto (f \longmapsto f(m)). \end{aligned}$$

De plus $\widehat{M}$ est quotient d'un module libre L. On a donc un morphisme injectif de $A-$module

$$M \longrightarrow \widehat{\widehat{M}} \longrightarrow \widehat{L}.$$

Comme $\widehat{L}$ est divisible, le lemme est démontré. □

Théorème 3.5.7. *Tout $A-$module est un sous $A-$module d'un module injectif.*

(dual de : tout $A-$module est quotient d'un module projectif).

Démonstration. Soit M un $A-$module. C'est un sous $A-$module divisible D. On a un morphisme de $A-$module

$$\begin{aligned} M &\longrightarrow Hom_{\mathbb{Z}}(A, D) \\ x &\longmapsto (a \longmapsto f(ax)). \end{aligned}$$

C'est un morphisme injectif. Comme D est divisible, $Hom_{\mathbb{Z}}(A, D)$ est un $A-$module injectif. □

Remarques 3.5.8. *On dit que la catégorie des $A-$module a assez d'injectifs. Ce n'est pas le cas dans toutes les catégories où la notion d'objet injectif a un sens.*

3.6 Homotopie de morphismes

Soient (E, d), (E', d') des complexes de $A-$modules. Soient $f, g : (E, d) \to (E', d')$ des morphismes de degré 0. On dit que f est homotope à g ssi il existe $h : E \to E'$ morphisme de complexes de degré 1 tel que, exposant $h : (h^n : E^n \to E^{n-1})$, on ait

$$f_n - g_n = d'^{(n-1)} h_n + h_{n+1} d^n.$$

On écrit alors $f \sim g$ (c'est une relation d'équivalence)

Proposition 3.6.1. *Si f et g sont homotopes, alors $H(f) = H(g) : H(E) \to H(E')$*

Démonstration. On a $f_n - g_n = 0$ sur $Z_n(E)$ et $\mathrm{Im}(f_n - g_n) \subset B_n(E')$. □

Soit M un $A-$module. Une résolution injective de M est une suite exacte

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

où I_n est un $A-$module injectif. Cela existe toujours car M est un sous-module d'un module injectif I^0. I^0/M est un sous-module d'un module injectif I^1. On a donc

$$0 \to M \to I^0 \to I^1.$$

$I^1/\mathrm{Im}(I_0)$ est un sous module d'un module injectif I^2. On obtient

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

On continue ainsi.

Une résolution injective n'est pas unique, et n'est pas unique à isomorphisme près.

Proposition 3.6.2. *Soit M un $A-$module. Soient deux complexes*

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & M & \longrightarrow & E^0 & \longrightarrow & E^1 & \longrightarrow & E^2 & \longrightarrow & \cdots \\ & & \varphi\downarrow & & & & & & & & \\ 0 & \longrightarrow & M' & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & I^2 & \longrightarrow & \cdots \end{array}$$

où le premier complexe est exact, φ est un morphisme de $A-$modules, I^n, pour $n \geq 0$ est un $A-$module injectif. Alors il existe un morphisme de complexes f prolongent φ. De plus, tout morphisme de complexes prolongeant φ est homotope à f. (on dit que f est unique à homotopie près)

Remarques 3.6.3. *On a un énonce dual. Soit*

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M' & \longrightarrow & 0 \\ & & & & & & & & \downarrow\varphi & & \\ \cdots & \longrightarrow & E_2 & \longrightarrow & E_1 & \longrightarrow & E_0 & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

(le complexe inférieur est exacte) un complexe avec P_n projectif. Alors, φ se prolonge en un morphisme de complexes. Le prolongement est unique à homotopie près.

3.7 Foncteur dérivés

Soient $\mathcal{C}$ et $\mathcal{D}$ des catégories. Ici $\mathcal{C} = \mathcal{D} = \mathcal{M}od(A)$ catégorie des $A-$modules avec A anneau commutatif. Mais ces concepts s'appliquent à toutes sortes de catégories. Soit $\mathcal{F}$ un foncteur de $\mathcal{C}$ vers $\mathcal{D}$. On dit que $\mathcal{F}$ est exact à gauche si pour toute exacte dans $\mathcal{C}$

$$0 \to M' \to M \to M'' \to 0$$

on a une suite exacte dans $\mathcal{D}$

$$0 \to \mathcal{F}(M') \to \mathcal{F}(M) \to \mathcal{F}(M'').$$

On dit que $\mathcal{F}$ est additif si $\mathcal{F}(f+g) = \mathcal{F}(f) + \mathcal{F}(g)$ pour f, g morphisme de $\mathcal{C}$.

On sait que $\mathcal{M}od(A)$ a assez d'injectifs. Soit M un $A-$module (un objet de $\mathcal{C}$). Soit

$$0 \to M \to I^0 \to I^1 \to \cdots$$

une résolution injective de M. Considérons le complexe

$$0 \to I^0 \to I^1 \to \cdots$$

On pose $R^n\mathcal{F}(M) = H^n(\mathcal{F}(I))$. On suppose $\mathcal{F}$ addictif et exact à gauche. On a un complexe

$$0 \to \mathcal{F}(I^0) \to \mathcal{F}(I^1) \stackrel{\delta^n}{\to} \mathcal{F}(I^2) \to \cdots$$

$R\mathcal{F}$ est le foncteur dérivé à droite de $\mathcal{F}$.

Proposition 3.7.1.

1. *$R^n\mathcal{F}$ est un foncteur addictif et $R^n\mathcal{F}$ ne dépend pas de la résolution choisie.*
2. *On a un isomorphisme de foncteurs $\mathcal{F} \simeq R^0\mathcal{F}$.*
3. *Si on a une suite exacte $0 \to M' \to M \to M'' \to 0$ de $A-$modules, on a un morphisme de foncteurs $\delta^n : R^n\mathcal{F}(M'') \to R^{n+1}\mathcal{F}(M')$ et une suite exacte*

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

4. *Si on a un morphisme de suite exactes courtes*

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

   on a un diagramme commutatif

$$\begin{array}{ccc} R^n\mathcal{F}(M'') & \xrightarrow{\delta^n} & R^{n+1}\mathcal{F}(M') \\ \downarrow & & \downarrow \\ R^n\mathcal{F}(N'') & \xrightarrow{\delta^n} & R^{n+1}\mathcal{F}(N'') \end{array}$$

5. *Si I est injectif et n entier> 0, on a $R^nF(I) = 0$.*

Démonstration.

1. Montrons l'indépendance de la résolution choisie. Soit une autre résolution

$$0 \to M \to I'^0 \to I'^1 \to \cdots,$$

on a

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & I'^0 & \longrightarrow & I'^1 & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & \cdots \end{array}$$

D'après la proposition précédente, ces résolution sont homotopies. Donc $H^n(F(I)) = H^n(F(I'))$.

2. On a $R^0\mathcal{F}(M) = \mathcal{F}(M)$ car $H^0(\mathcal{F}(I)) = \mathcal{F}(M)$.

3. Soient I et I'' des résolutions injectives de M' et M''. On a

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & \overset{\alpha}{\swarrow} & \downarrow{\scriptstyle ?} & \overset{\beta}{\searrow} & \downarrow & & \\ 0 & \longrightarrow & I'^0 & \longrightarrow & I'^0 \oplus I''^0 & \longrightarrow & I''^0 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

Comme I'^0 est injectif, on a morphisme $\alpha : M \to I'^0$ et un morphisme $\beta : M \to I''^0$. D'où $\alpha \oplus \beta : M \to I'^0 \oplus I''^0$, qui est injectif. On a $N' : \operatorname{coker}(M' \to I'^0)$ idem pour N et N''.

On repéte la construction pour $0 \to N' \to N \to N'' \to 0$. Cela donne

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I'^0 & \longrightarrow & I^0 & \longrightarrow & I''^0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I'^1 & \longrightarrow & I^1 & \longrightarrow & I''^1 & \longrightarrow & 0
\end{array}$$

avec I'^1, I^1, I''^1 injectifs et on obtient une suite exacte de résolutions injectives. On utilise le lemme du serpent pour défini $\delta^n = H^n(I'') \to H^{n+1}(I')$.

4. Compliqué mais direct.

5. Si I est injectif, on a la résolution $0 \to I \to I \to 0 \to 0$. Donc $R^n\mathcal{F}(I) = 0$ si $n > 0$.

□

On a une notion duale du foncteur dérivé à droite. On suppose que $\mathcal{F}$ contravarient, addictif et exact à droite : pour toute suite exacte $0 \to M' \to M \to M'' \to 0$, on a une suite exacte

$$\mathcal{F}(M'') \to \mathcal{F}(M) \to \mathcal{F}(M') \to 0.$$

Dans $\mathcal{C}$, il y a assez de projectifs. Soit M un $A-$module. Il existe une résolution projective de $\mathcal{C}$

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

qui donne lieu à une suite exacte

$$0 \to \mathcal{F}(M) \to \mathcal{F}(P_0) \to \mathcal{F}(P_1) \to \cdots$$

On pose $R^n\mathcal{F}(P) = H^n(\mathcal{F}(P))$. C'est le foncteur dérivé à gauche de $\mathcal{F}$.

Il y a une proposition analogue à la précédente : 1., 2., 3., 4. et où 5. devient
5. Si P est projectif et $n \geq 1$, on a $R^n\mathcal{F}(P) = 0$.

3.8 Les foncteurs Ext et Tor

Ext provient de extension.
Tor provient de torsion.

Soit M un $A-$module. Considérons le foncteur de $\mathcal{M}od(A)$ vers $\mathcal{M}od(A)$ qui à N associe $Hom_A(M,N)$. C'est un fonction addictif, covariant et exact à gauche. (Si on a une suite exacte $0 \to N' \to N \to N'' \to 0$, on en déduit une suite exacte $0 \to Hom_A(M,N') \to Hom_A(M,N) \to Hom(M,N'')$) On note ce foncteur $Hom_A(M,\cdot)$. On pose pour n entier≥ 0.

$$R^n Hom_A(M,\cdot)(N) = Ext^n(M,N).$$

C'est le foncteur Ext^n.

Autre construction. Fixons un $A-$module N, considérons le foncteur addictif, contravariant, exact à droite qui à M associé $Hom(M,N)$. On le note $Hom_A(\cdot,N)$. On peut considérer $R^n Hom_A(\cdot,N)(M)$. On obtient encore $Ext^n(M,N)$ (pas évident). On a $Ext^0(M,N) = Hom_A(M,N)$.

Une extension de N par M est une suite exacte courte $0 \to N \to E \to M \to 0$. (dans la catégorie des $A-$modules) Deux extensions $0 \to N \to E \to M \to 0$ et $0 \to N \to E' \to M \to 0$ sont équivalentes si on a un isomorphisme de complexes qui est l'identité sur N et M. On a l'extension

$$0 \to N \to N \oplus M \to M \to 0$$

Les extensions triviales sont celles qui sont équivalentes à $0 \to N \to N \oplus M \to M \to 0$.
L'équivalence des extensions est une relation d'équivalence. Si $0 \to N \to E \to M \to 0$ et $0 \to N \to E' \to M \to 0$ sont deux extensions, on peut considérer leur somme défini par

$$0 \to N \to E \oplus_M E' \to M \to 0$$

où $E \oplus_N E' = \{(e,e') \in E \times E' \mid g(e) = g'(e')\}$. Cette loi défini une loi de groupe sur les classe d'équivalence d'extension. La classe de l'extension triviale est l'élément neutre.

Exemples 3.8.1. $A = \mathbb{Z}$ les extensions

$$0 \to \mathbb{Z}/2\mathbb{Z} \stackrel{\times 2}{\to} \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

(trivial) ne sont pas équivalence.

Proposition 3.8.2. *On a une bijection $Ext^1(M,N) \simeq$classe d'équivalence d'extension de N par M. (et même un isomorphisme de groupes)*

Démonstration. Soit $0 \to N \to E \to M \to 0$ une extension. On a une suite exacte longue

$$0 \to \underset{\| \\ Ext^0(M,N)}{Hom_A(M,N)} \to \underset{\| \\ Ext^0(M,E)}{Hom_A(M,E)} \to \underset{\| \\ Ext^0(M,M)}{Hom_A(M,M)} \xrightarrow{\delta} Ext^1(M,N)$$

Comme $id_M \in Hom_A(M,M)$, on a $\delta(id_M) \in Ext^1(M,N)$ (ne dépend pas que de la classe d'équivalence). Réciproquement, soit un élément de $Ext^1(M,N)$. Soit $0 \to N \to I^0 \to I/Q \to 0$ une suite exacte avec I^0 injectif et $Q = \operatorname{Im} N$. On en déduit

$$0 \to Hom(M,N) \to Hom(M,I^0) \to Hom(M,I^0/Q) \to Ext^1(M,N) \to Ext^1(M,I^0) \to 0$$

car I^0 injectif. Comme la suite est exacte, il exacte $\varphi \in Hom(M,I^0/Q)$ bien défini à $Hom(M,I^0)$ près. Alors on a

$$0 \to N \to I^0 \oplus_{I^0/Q} M \to M \to 0$$

où $I^0 \oplus_{I^0/Q} M = \{(i,m) \in I^0 \times M \mid \varphi(i) = \text{classe de } m \text{ dans } I^0/Q\}$. On a bien une extension de N par M. Ces deux construction sont inverses l'une de l'autre. □

Fixons un $A-$module M. Le foncteur $M \otimes_A \cdot$ de la catégorie des $A-$modules vers elle-même est covarient, additif. Il associe à N le $A-$module $M \otimes_A N$.

Proposition 3.8.3. *$M \otimes_A \cdot$ est exacte à droite.*

Démonstration. Soit $0 \to N' \to N \to N'' \to 0$ une suite exacte courte de $A-$modules. Il faut montrer que $M \otimes_A N' \to M \otimes_A N \to M \otimes_A N'' \to 0$ est exacte. Il faut montrer l'exactitude en $M \otimes_A N$.
Soit $f : {}^{M \otimes_A N}\Big/_{\operatorname{Im}(M \otimes_A N')} \to M \otimes_A N''$. Construisons sa réciproque. Soit $m \in M$. Soit $n'' \in N''$. Il existe $n \in N$ d'image n'' dans N''. On pose

$$\begin{aligned} g : M \times N'' &\longrightarrow {}^{M \otimes_A N}\Big/_{\operatorname{Im}(M \otimes_A N')} \\ (m,n'') &\longmapsto \text{classe de } m \otimes n. \end{aligned}$$

C'est bien défini car si m_1 et $m_2 \in N$ ont pour image n'' dans N'', on a $n_1 - n_2 \in \ker \varphi = \operatorname{Im} \psi$. Posons $n_1 - n_2 = \psi(n')$. Donc $m \otimes n_1 - m \otimes n_2 = m \otimes (n_1 - n_2) = m \otimes \psi(n') \in \operatorname{Im}(M \otimes_A N')$. De plus g est réciproque de f. □

On pose $R^n(M \otimes_A \cdot)(N) = Tor^n(M, N)$ (foncteur dérivé à gauche). C'est le n-ème groupe d'homotogie du complexe

$$\cdots \to M \otimes P_2 \to M \otimes P_1 \to M \otimes P_0 \to 0$$

où

$$\cdots P_2 \to P_1 \to P_0 \to N \to 0$$

est une résolution projective de N.

Comme $M \otimes_A N \simeq N \otimes_A M$, on a $Tor^n(M, N) \simeq Tor^n(N, M)$.

3.9 Modules plats

Soit A un anneau commutatif. Soit M un $A-$module.

Proposition 3.9.1. *Les assertion suivantes sont équivalentes*

1. *Pour toute suite exacte $N' \to N \to N''$ de $A-$modules, la suite $N' \otimes M \to N \otimes M \to N'' \otimes M$ est exacte.*

2. *Pour toute suite exacte courte $0 \to N' \to N \to N'' \to 0$ de $A-$modules, la suite $0 \to N' \otimes M \to N \otimes M \to N'' \otimes M \to 0$ est exacte.*

3. *Pour toute suite exacte $0 \to N' \to N$ de $A-$modules, la suite $0 \to N' \otimes M \to N \otimes M \to$ est exacte.*

Démonstration. 1.⇒ 2., 2.⇒ 3. OK. Pour 3.⇒ 1. cela résulte de $\cdot \otimes_A M$ est exacte à droite. □

Lorsque 1., 2., 3. sont vérifiés, on dit que M est un $A-$module plat.

Tout module projectif est plat. Soit $M = \bigoplus_{i \in I} M_i$ une somme directe de $A-$modules. C'est un module plat ssi M_i est plat pour tout $i \in I$.

3.10 Homologie et cohomologie des groupes

Soit G un groupe. Soit $\mathbb{Z}[G]$ l'anneau en groupe associé à G. Il est abélien si et seulement si G est commutatif. Soit M un groupe abélien. On dit que c'est un $G-$module si M est muni d'une action de G et qu'on a, pour tous m_1, $m_2 \in G$, $g(m_1 + m_2) = gm_1 + gm_2$. (On a la notion analogue pour les modules suites)

Il revient au même de dire que M est au $\mathbb{Z}[G]-$module à gauche. Ici les modules sont des modules à gauche. Un morphisme de groupes $M \to N$ entre $G-$modules est un morphisme de $G-$modules si, pour tout $m \in M$, $g \in G$, on a $\varphi(g \cdot m) = g \cdot \varphi(m)$. On obtient la catégorie des $G-$modules.

On a les notions de complexe, suite exacte, objets injectif, projectif ,libre ,homologie, foncteur dérivé.

Soit M un $G-$module. On pose

$$M^G = \{m \in M \mid \textit{pour tout } g \in G,\ g \cdot m = m\}.$$

(plus grand sous-groupe de M sur lequel G opère trivialement).

Alors $M \to M^G$ est un foncteur de la catégorie des $G-$modules vers la catégorie des groupes abéliens.

Si on a une suite exacte de $G-$modules,

$$0 \to M' \to M \to M'' \to 0,$$

on en déduit

$$0 \to M'^G \to M^G \to M''^G.$$

Donc le foncteur est exact à gauche. M^G est le groupe des invariants de M sous G.

On pose $M_G = {}^{M}\Big/\{g \cdot m - m \mid g \in G,\ m \in M\}$. C'est le groupe des coinvariants de M sous G. C'est le plus grand quotient de M sur lequel G opère trivialement. $M \to M_G$ est un foncteur de la catégorie des $G-$modules vers la catégorie des groupes abéliens.

Si $0 \to M' \to M \to M'' \to 0$ est une suite exacte de $G-$modules, on a une suite exacte de groupes

$$M'_G \to M_G \to M''_G \to 0.$$

Donc le foncteur des coinvariants est exact à droite.

Exemples 3.10.1. de $G-$modules

· 0 ; $\mathbb{Z}[G]$(mini de l'action $g \cdot [h] = [gh]$) ;

· $\mathbb{Z}[X]$ où X est un ensemble muni d'une action de G (avec $g \cdot [x] = [gx]$ pour $g \in G$, $x \in X$) ;

· $\mathbb{Z}$ muni de l'action triviale de G.

· Si M et N sont deux $G-$modules, $Hom_{groupe}(M, N)$ est un $G-$module par

$$(g \cdot \varphi)(m) = g(\varphi(g^{-1} \cdot m)) \qquad (g \in G,\ m \in M,\ \phi \in Hom_{groupe}(M, N)).$$

De même, $M \otimes N$ est un $G-$module. Alors $Hom_G(M, N) = \big(Hom_{groupe}(M, N)\big)^G$. On a, pour M $G-$module, $\underset{\varphi(1) \leftarrow \varphi}{M^G \simeq Hom_G(\mathbb{Z}, M)}$. On a de plus $M_G \simeq M \otimes_{\mathbb{Z}[G]} \mathbb{Z}$. On peut considérer les foncteurs dérivés :

$$H^n(G, M) = R^n \underbrace{\begin{pmatrix} foncteur\ des \\ invariants\ sous\ G \end{pmatrix}}_{dérivé\ à\ droite}$$
$$\simeq Ext^n_G(\mathbb{Z}, M).$$

C'est le $n-$ème groupe de cohomologie du $G-$module M. De même

$$H_n(G, M) = R^n \underbrace{\begin{pmatrix} foncteur\ des\ coin- \\ variants\ sous\ G \end{pmatrix}}_{dérivé\ à\ gauche}$$
$$\simeq Tor^G_n(\mathbb{Z}, M).$$

C'est le $n-$ème groupe d'homologie du $G-$module M.

Pour calculer ces groupes, on peut utiliser des résolutions projectifs, par exemple, libres de G.

Pour i entier≥ 0, on a l'action diagonale de G sur G^{i+1} donnée par

$$g \cdot (g_0, g_1, \cdots, g_i) = (gg_0, gg_1, \cdots, gg_i).$$

Posons $P_i = \mathbb{Z}[G^{i+1}]$. C'est un $G-$module, on a

$$\begin{aligned} d_i : P_{i+1} &\longrightarrow P_i \\ (g_0, \cdots, g_i) &\longmapsto \sum_{j=0}^{i} (-1)^j (g_0, \cdots, \widehat{g_j}, \cdots, g_i). \end{aligned}$$

(Rappel : $(g_0, \cdots, \widehat{g_j}, \cdots, g_i) = (g_0, \cdots, g_{i-1}, g_{i+1}, \cdots, g_i)$)

On pose

$$\begin{aligned} d_0 : P_0 = \mathbb{Z}[G] &\longrightarrow \mathbb{Z} \\ [g] &\longmapsto 1. \end{aligned}$$

Le noyau de d_0 est I_G l'idéal d'augmentation de $\mathbb{Z}[G]$. C'est un idéal bilatère. d_0 s'appelle l'application d'augmentation.

Le $G-$module P_i est libre. En effet, il a pour base $(1, g_1, \cdots, g_i)$ pour $g_1, \cdots, g_i \in G^i$. D'où une résolution libre du $G-$module $\mathbb{Z}$.

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} \mathbb{Z} \to 0.$$

On pose $K = Hom_G(P_i, M)$. On a $f \in K_i$ ssi pour tout $g \in G$ et tout $(g_0, \cdots, g_i) \in G^{i+1}$, on a $f(g(g_0, \cdots, g_i)) = gf(g_0, \cdots, g_i)$ et f morphisme de groupe $P_i \to M$.

Donc f est déterminé par $f(1, g_1, \cdots, g_i)$ (car f morphisme de $G-$module).

On peut définir le cobord de $f \in K_i$. f est déterminé par $f(1, g_1, g_1g_2, \cdots, g_1g_2 \cdots g_i)$. Posons $\varphi(g_1, \cdots, g_i) = f(1, g_1, g_1g_2, \cdots, g_1g_2 \cdots g_i)$. Déterminons le cobord de φ. On a $d\varphi : G^{i+1} \to$

M, où

$$\begin{aligned} d\varphi(g_1,\cdots,g_{i+1}) = g_1\varphi(g_2,\cdots,g_{i+1}) & \\ +\sum_{j=1}^{i}(-1)^j\varphi(g_1,\cdots,g_{j-1},g_jg_{j+1},g_{j+2},\cdots,g_{i+1}) & \\ +(-1)^{i+1}\varphi(g_1,\cdots,g_i). & \end{aligned}$$

On a $H^i(G,M) = {Z^i(G,M)}\Big/{B^i(G,M)}$ où $Z^i(G,M)$ est le groupe des $i-$ *cocycles* et $B^i(G,M)$ est le groupe des $i-$cobords.

On a $Z^i(G,M) = \ker d^i$, $B^i(G,M) = \operatorname{Im} d^{i-1}$.

3.11 Quelques groupes d'homologie et cohomologie

Soit G un groupe. Soit M au $G-$module. On a $H^0(G,M) = M^G$ (0-cocycles) et on a $H^1(G,H) = {Z^1(G,M)}\Big/{B^1(G,M)}$. Avec

$$Z^1(G,M) = \{\varphi : G \to M \mid \textit{pour tous } g,g' \in G, \textit{ on a } \varphi(gg') = g\cdot\varphi(g') + \varphi(g)\}$$

et

$$B^1(G,M) = \{\varphi : G \to M \mid \textit{il existe } m \in M \textit{ avec } \varphi(g) = g\cdot m - m\}.$$

On a vu que

$$H^1(G,M) = Ext^1_G(\mathbb{Z},M) = \{\textit{extension } 0 \to M \to E \to \mathbb{Z} \to 0\}\Big/_{\textit{équivalence}}.$$

On dit que $H^1(G,M)$ paramètre les extensions de $\mathbb{Z}$ par M (dans la catégorie des $G-$modules).

Si G opère trivialement sur M, on a

$$\begin{aligned} Z^1(G,M) &= \{\varphi : G \to M \mid \varphi(gg') = \varphi(g) + \varphi(g')\} \\ &= Hom_{groupe}(G,M) \\ B^1(G,M) &= \{0\}. \end{aligned}$$

Donc $H^1(G,M) \simeq Hom_{groupe}(G,M)$. En particulier, dans ce cas, $H^1(G,M)$ ne dépend que de $G^{ab} = {}^{G}\Big/_{[G,G]}$ où $[G,G]$ =sous groupe de G engendré par les communitateurs, c'est à dire $\{ghg^{-1}h^{-1} \mid g,h \in G\}$. G^{ab} est le plus grand quotient abélien de G.

On a

$$Z^2(G,M) = \{\varphi : G^2 \to M \mid \textit{pour tous } g,g',g'' \in G, \textit{ on a } g\varphi(g',g'') - \varphi(gg',g'') + \varphi(g,g'g'') - \varphi(g,g') = 0\}$$

et

$$B^2(G,M) = \{\varphi : G^2 \to M \mid \textit{il existe } \psi : G \to M \textit{ avec } \varphi(g,g') = \psi(gg') - g\psi(g') + \psi(g)\}.$$

On pose $M \rtimes G = M \times G$ muni de la loi de groupe $((m,g),(m',g')) \mapsto (m + gm', gg')$. C'est le produit semi-direct de M et G. C'est un groupe. On a une suite exacte de groupes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & M \rtimes G & \longrightarrow & G & \longrightarrow & 0 \\ & & m & \longmapsto & (m,1) & & & & \\ & & & & (m,g) & \longmapsto & g. & & \end{array}$$

Pour $g \in G$ et $(m,1) \in M \rtimes G$, on a $(0,g)(m,1)(0,g)^{-1} = (gm,g)(0,g^{-1}) = (gm,1)$. Donc la conjugation par $0 \times G$ dans $M \times \{1\} \subset M \rtimes G$ redonné l'action de G sur M.

Une extention de G par M est une suite exacte de groupes

$$0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 0$$

telle que la conjugasion par $e \in E$ de $i(m)$, pour $m \in M$, soit $i(\pi(e) \cdot m)$. C'est-à-dire, on a

$$ei(m)e^{-1} = i(\pi(e) \cdot m).$$

Deux telles extensions sont équivalentes si on a

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 0 \\ & & \| & & & & \| & & \\ 0 & \longrightarrow & M & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

et un isomorphisme $E \simeq E'$ compatible au diagramme. C'est un relation d'équivalence. Une extension est dit triviale si elle est équivalente au produit semi-directe.

Exercice 3.11.1. Définir la somme de deux extensions.

Théorème 3.11.2. *On a une bijection*

$$H^2(G,M) = \underbrace{\{extensions\ de\ G\ par\ M\}}_{\| \mathscr{E}}/équivalence\ .$$

Démonstration. Décrivons $\mathscr{E}$ comme ensemble. Soit $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 0$ une extension de G par M. Soit $s : G \to E$ une section de π. On a

$$\begin{aligned} E &\to \bigsqcup_{g\in G} i(M)\cdot s(g) \\ &\simeq M \times G. \end{aligned}$$

où $i(M)\cdot s(g) = \pi^{-1}(g)$.

Pour $g_1, g_2 \in G$, on $s(g_1)s(g_2) \in \pi^{-1}(g_1g_2)$ car $\pi \in Hom(E,G)$. Donc il existe $c(g_1,g_2) \in M$ tels que $s(g_1)s(g_2) = i(c(g_1,g_2))s(g_1g_2)$.

On a $s(1)s(1) = i(c(1,1))s(1)$. Donc $s(1) = i(c(1,1))$. On a donc $c : G\times G \to M$ qui vérifie $(m,g)(m',g') = (m + gm' + c(g,g'), gg')$ (on utilise $M\times G \simeq E$) car

$$\begin{aligned} i(m)s(g)i(m')s(g') &= i(m)s(g)i(m')s(g)^{-1}s(g)s(g') \\ &= i(m)i(g\cdot m')i(c(g,g'))s(gg') \\ &= i(m+gm'+c(g,g'))s(gg'). \end{aligned}$$

Utilisons que la loi de groupe est associative dans E. On a

$$\begin{aligned} (m,g)(m',g')(m'',g'') &= (m+gm'+c(g,g')+gg'm''+c(gg',g''), gg'g'') \\ &= (m+g(m'+g'm''+c(g'g''))+c(g,g'g''), gg'g'') \\ &= (m,g)((m',g')(m'',g'')). \end{aligned}$$

Donc

$$c(gg',g'') + c(g,g') - gc(g,g') - c(g,g'g'') = 0.$$

Précisement la relation de 2−cocycle. $c \in Z^2(G, M)$.

Vérifions que la classe de c dans $H^2(G, M)$ ne dépend pas du choix de s.

Posons $s' = ts$ avec $t : G \to M$. On a $c' : G \times G \to M$ donnée par

$$\begin{aligned} c'(g_1, g_2) &= s'(g_1)s'(g_2)s'(g_1g_2)^{-1} \\ &= t(g_1)s(g_1)t(g_2)s(g_2)s(g_1g_2)^{-1}t(g_1g_2)^{-1} \\ &= t(g_1)s(g_1)t(g_2)s(g_1)^{-1}s(g_1)s(g_2)s(g_1g_2)^{-1}t(g_1g_2)^{-1} \\ &= t(g_1)(g_1 \cdot t(g_2))c(g_1, g_2)t(g_1, g_2)^{-1}. \end{aligned}$$

Donc

$$c'(g_1, g_2) = t(g_1) + g_1t(g_2) - t(g_1g_2) + c(g_1, g_2).$$

Donc

$$c'(g_1, g_2) - c(g_1, g_2) = \underbrace{t(g_1) + g_1 \cdot t(g_2) - t(g_1g_2)}_{2-cobord}.$$

Donc les classes de c et c' dans $H^2(G, M)$ coïncident. On a trouvé $\mathscr{E} \to H^2(G, M)$.

Établissons la réciproque. Soit $c : G \times G \to M$ un 2−cocycle. On a une loi de groupe sur $M \times G$ donnée par $(m, g)(m', g') = (m + gm' + c(g, g'), gg')$. L'élément neutre est $(-c(1, 1), 1)$. On a

$$\begin{aligned} i : M &\longrightarrow E \\ m &\longmapsto (m - c(1, 1), 1) \end{aligned}$$

et

$$\begin{aligned} \pi : E &\longrightarrow G \\ (m, g) &\longmapsto g. \end{aligned}$$

L'inverse de (m, g) est $(-gm - c(g^{-1}, g) - c(1, 1), g^{-1})$. Donc on a bien une extension de G par M. Si c'est un autre 2−cocycle tel que c, c' est un 2−cobord, l'extension associé à c' est

équivalente à celle associé à c.

On a $c' = c + dt$ où $t : G \to H$. Et on a l'équivalence $(m, g) \mapsto (m + t(g), g)$. D'où une application $K^2(G, M) \to \mathscr{E}$. (réciproque de la précédente). □

Le groupe $H_n(G, M)$ est donné par l'homologie du complexe

$$\cdots \longrightarrow P_2 \otimes M \longrightarrow P_1 \otimes M \longrightarrow P_0 \otimes M \longrightarrow 0$$

où

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

est la résolution standard de $\mathbb{Z}$ comme $G-$module.

On a $H_0(G, M) = M_G = {}^{M}\!/_{I_G M}$ où I_G :idéal d'augmentation de $\mathbb{Z}[G]$. On a une suite exacts de $G-$modules

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0.$$

On en déduit une suite exacte longue

$$0 = H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to \underset{\simeq I_G/I_G^2}{H_0(G, I_G)} \to \underset{\substack{\simeq \mathbb{Z}[G]/I_G \\ \simeq \mathbb{Z}}}{H_0(G, \mathbb{Z}[G])} \simeq \underset{\simeq \mathbb{Z}}{H_0(G, \mathbb{Z})} \to 0.$$

Proposition 3.11.3. *On a les isomorphismes de groupes*

$$H_1(G, \mathbb{Z}) \simeq {}^{I_G}\!\Big/_{I_G^2} \simeq G^{ab}.$$

Démonstration. Le premier isomorphisme se déduit de la suite exacte longue. Vérifions le deuxième isomorphisme. Considérons

$$\begin{aligned} f : G &\longrightarrow {}^{I_G}\!\Big/_{I_G^2} \\ g &\longmapsto \textit{classe de } [g] - [1]. \end{aligned}$$

C'est un morphisme de groupes

$$\begin{aligned} f(gg') - f(g)f(g') &= [gg'] - [1] - ([g] - [1]) - ([g'] - [1]) \\ &= [g][g'] - [g] - [g'] + [1] \\ &= ([g] - [1])([g'] - [1]) \in I_G^2. \end{aligned}$$

Comme $I_G \Big/ I_G^2$ est un groupe abélien, on obtient $\bar{f} : G^{ab} \to I_G \Big/ I_G^2$. $\bar{f}$ est surjectif car I_G est engendré par $\{[g] - [1] \mid g \in G\}$. Le noyau de $\bar{f}$ est l'image réciproque de I_G par f.

I_G^2 est engendré par $\{([g] - [1])([g'] - [1]) \mid g, g' \in G\}$.

Or $([g] - [1])([g'] - [1]) = [gg'] - [g] - [g'] + [1]$.

(à finir...) □

On sait que f est un morphisme surjectif de groupes. On considère

$$\begin{aligned} I_G &\longrightarrow G^{ab} \\ [g] - [1] &\longmapsto \textit{classe } \bar{g} \textit{ de } g \textit{ dans } G^{ab}. \end{aligned}$$

Comme I_G est le groupe abélien librement engendré par $[g]-[1]$, $g \in G\backslash\{1\}$, u est uniquement défini comme morphisme de groupes/ Comme u est surjectif et réciproque de f, il reste à montrer que $u(I_G^2) = \{1\}$. Cela résulte de

$$\begin{aligned} u(([g] - [1])([h] - [1])) &= u([gh] - 1 - ([g] - [1]) - ([h] - [1])) \\ &= \overline{gh}\bar{g}^{-1}\bar{h}^{-1} \\ &= \overline{ghg^{-1}h^{-1}} \\ &= 1. \end{aligned}$$

3.12 Changement de groupe

Soit G un groupe. Soit H un sous-groupe de G. Soit N un $H-$module. Rappelons que tout $G-$module est un $H-$module, en particulier $\mathbb{Z}[G]$.

Posons $M = Hom_H(\mathbb{Z}[G], N)$. C'est un $G-$module (pour l'action $g \cdot \varphi(h) = \varphi(hg^{-1})$, $g \in G$, $\varphi \in M$).

Proposition 3.12.1. *(lemme de Shapiro) On a* $H^i(G,M) \simeq H^i(H,N)$ *et* $H_i(G,M) \simeq H_i(H,N)$ *(isomorphisme de groupes pour tout* $i \geq 0$*).*

Démonstration. Soit P une résolution libre de $\mathbb{Z}$ comme $G-$module. C'est aussi une résolution libre de $\mathbb{Z}$ comme $H-$module. Donc les complexes $Hom_G(P,M)$ et $Hom_H(P,N)$ coïncident. Donc les groupes de cohomologie coïncident.

De même pour l'homologie. □

Soit T un groupe abélien, $Hom(\mathbb{Z}[G],T)$ est un $G-$module (comme ci-dessus). Un $G-$module isomorphe à un module de ce type est dit coinduit. Un $G-$module isomorphe à un module du type $T \otimes \mathbb{Z}[G]$ est dit induit.

Soit M un $G-$module. On a la suite exacte de $G-$modules

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

qui donne

$$0 \longrightarrow M \otimes I_G \longrightarrow M \otimes \mathbb{Z}[G] \longrightarrow M \longrightarrow 0.$$

On a $H^i(G, M \otimes \mathbb{Z}[G]) = 0$ pour tout $i \geq 1$. On a la suite exacte longue qui donne

$$H^i(G, M \otimes \mathbb{Z}[G]) \longrightarrow H^i(G,M) \longrightarrow H^{i+1}(G, M \otimes I_G) \longrightarrow H^{i+1}(G, M \otimes \mathbb{Z}[G]).$$

($\mathbb{Z}[G]$ et I_G sont des $\mathbb{Z}-$module libres)

On peut démontrer des propriétés de H^i grâce des propriété de H^{i+1} (et réciproquement). C'est le décalage du degré.

De même on a

$$\begin{array}{ccccccc} 0 & \longrightarrow & M & \longrightarrow & Hom(\mathbb{Z}[G],M) & \longrightarrow & M' \longrightarrow 0 \\ & & m & \longmapsto & ([g] \mapsto g \cdot m) & & \end{array}$$

Donc $H_{i+1}(G,M') \simeq H_i(G,M)$.

Soit $f : H \to G$ un morphisme de groupes (H n'est pas forcément un sous-groupe de G). Soient Q et P les résolutions standards de $\mathbb{Z}$ comme H et $G-$module respectivement. On a un morphisme de complexes $Q \to P$ qui se déduit de f. Soit M un $G-$module. C'est un $H-$module par $h \cdot m = f(h) \cdot m$. Alors on déduit de f :

$$f^* : H^i(G, M) \longrightarrow H^i(H, M)$$

(contravatiant).

Si f est l'injection $H \hookrightarrow G$, alors on pose $f^* = Res : H^i(G, M) \to H^i(H, M)$ restriction. Si $f : H \to G \simeq {}^{H}/_{K}$ est surjective, M^K est un ${}^{H}/_{K}$ −module. On a $H^i\left({}^{H}/_{K}, M^K\right) \to H^i(H, M^K) \to H^i(H, M)$. On pose $Inf : H^i\left({}^{H}/_{K}, M^K\right) \to H^i(H, M)$ inflation.

Revenons à un morphisme de groupes $f : H \to G$. On a de même $f_* : H_i(H, M) \to H_i(G, M)$ (covariant). En particulier, si $f : H \hookrightarrow G$ (inclusion), on pose $Cor : H_i(H, M) \to H_i(G, M)$ corestriction.

3.13 Cohomologie des groupes fini

Soit G un groupe fini de cardinal $|G|$. On pose $N_G = \sum_{g \in G}[g] \in \mathbb{Z}[G]$, c'est le norme. On a $N_G I_G = 0$ car pour $h \in G$,

$$N_G([h] - [1]) = \sum_g [gh] - \sum_g [g] \overset{G \text{ groupe}}{=\!=\!=} 0.$$

On a $I_G N_G = 0$ de même.

Soit M un $G-$module. On a

$$\begin{aligned} N_G : M &\longrightarrow M \\ m &\longmapsto N_G \cdot m. \end{aligned}$$

On a $I_G M \subset \ker N_G = M[N_G]$ et $N_G M \subset M[I_G]$ où

$$M[I] = \{m \in M \mid Im = 0\} \text{ pour } I \subset \mathbb{Z}[G].$$

On en déduit

$$N_G^* : \underset{\substack{\| \\ M/I_G M}}{H_0(G,M)} \longrightarrow \underset{\substack{\| \\ M^G = M[I_G]}}{H^0(G,M)}.$$

On pose $\hat{H}_0(G,M) = \ker N_G^*$ et $\hat{H}^0(G,M) = {}^{M^G}\!/_{N_G M}$. Comme G est fini, on a un isomorphisme de $G-$module, pour T groupe abélien

$$\begin{aligned} Hom(\mathbb{Z}[G], T) &\simeq T \otimes \mathbb{Z}[G] \\ \varphi \qquad &\mapsto \sum_{g \in G} \varphi(g) \otimes [g]. \end{aligned}$$

Pour un groupe fini, être induit équivaut à être coinduit.

Proposition 3.13.1. *Si G est induit, on a $\hat{H}_0(G,M) = 0$ et $\hat{H}^0(G,M) = 0$.*

Démonstration. Posons $M = T \otimes \mathbb{Z}[G]$. Soit $x = \sum_{g \in G} t_g \otimes g$. Si $x \in M^G$, $g \mapsto t_g$ est constant. Donc $x = t_1 \otimes (\sum [g]) = t_1 \otimes N_G = N_G(t_1 \otimes 1)$. Donc $x \in \operatorname{Im} N_G$. Donc $\hat{H}^o(G,M) = 0$.

De même, si $N_G(\sum_g t_g \otimes [g]) = 0$, on a $\sum_g t_g = 0$ et donc $\sum_g t_g \otimes g = \sum_g t_g \otimes ([g]-[1]) \in I_G M$. Donc $\hat{H}_0(G,M) = 0$. □

On pose

$$\begin{cases} \hat{H}^i(G,M) = H^i(G,M) & i \geq 1 \\ \hat{H}^{-1}(G,M) = \hat{H}_0(G,M) & i = -1 \\ \hat{H}^i(G,M) = H_{-1-i}(G,M) & i \leq -2 \end{cases}.$$

Ce sont les groupes de cohomologie modifiés de Tate.

Théorème 3.13.2. *Soit $0 \to M' \to M \to M'' \to 0$ une suite exacte de $G-$modules, on a une suite exact longue*

$$\cdots \hat{H}^i(G,M') \longrightarrow \hat{H}^i(G,M) \longrightarrow \hat{H}^i(G,M'') \xrightarrow{\hat{\delta}} \hat{H}^{i+1}(G,M').$$

qui prolonge les suites exactes d'homologie et de cohomologie déjà connues.

Démonstration. On dispose de

$$\begin{array}{ccccccccccc}
\longrightarrow & H_1(G,M'') & \xrightarrow{\delta} & H_0(G,M') & \longrightarrow & H_0(G,M) & \longrightarrow & H_0(G,M'') & \longrightarrow & 0 & \\
& \downarrow & & \downarrow{\scriptstyle N_G} & & \downarrow{\scriptstyle N_G} & & \downarrow{\scriptstyle N_G} & & \downarrow & \\
& 0 & \longrightarrow & H^0(G,M') & \longrightarrow & H^0(G,M) & \longrightarrow & H^0(G,M'') & \longrightarrow & H^1(G,M') & \longrightarrow
\end{array}$$

Ce diagramme est commutatif. Montrons le pour le carré à droite. Soit $m'' \in M''$. Soit $m \in M$ d'image m'' dans $H_0(G,M'') = {}^{M''}\!/_{I_G M''}$. On lui encore la $1-$cocycle $g \mapsto gm - m$ et dont la classe est $\delta(\overline{m''})$. Si $m'' = N_G n''$. Il existe $m \in M$ tel que $m = N_G n$. Donc le cocycle est nul, donc $\delta(\overline{m''}) = 0$. D'où la commutativité. Démonstration analogue pour le carré de gauche.

Il reste à défini $\hat{\delta}$ pour $i = 0$. On applique le lemme du serpent au diagramme ci-dessus. □

Remarques 3.13.3. *Soit P une résolution libre de $\mathbb{Z}$, par des $G-$modules de type fini. (Par exemple la résolution standard si G est fini) Posons $P^* = Hom(P,\mathbb{Z})$, on pose $P_{-i} = Hom(P_{i-1},\mathbb{Z})$ pour $i \geq 1$. On a*

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\varepsilon} P_0^* \longrightarrow P_1^* \longrightarrow P_2^* \longrightarrow \cdots$$

On en déduit

$$\cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow P_{-1} \longrightarrow P_{-2} \longrightarrow \cdots$$

Alors $\hat{H}^i(G,M)$ provient de la cohomologie du complexe

$$\cdots \longrightarrow Hom_G(P_{-1},M) \longrightarrow Hom_G(P_0,M) \longrightarrow Hom_G(P_1,M) \longrightarrow \cdots$$

Soit H un sous-groupe de G. Pour $i \geq 0$, on a $Res : H^i(G,M) \to H^i(H,M)$. Elle commute à S.

Par décalage on a $H^i(G,M) = H^{i+1}(G,M')$ et donc $\hat{H}^i(G,M) = \hat{H}^{i+1}(G,M')$ (car pour M induit $\hat{H}^i(G,M) = 0$). Par décalage, la restriction est défini : $\hat{H}^i(G,M) \to \hat{H}^i(H,M)$ pour $i \in \mathbb{Z}$. De même la corestriction : $\hat{H}^i(H,M) \to \hat{H}^i(G,M)$ est défini pour $i \in \mathbb{Z}$.

Proposition 3.13.4. *1.* $Res : \hat{H}_0(G, M) \to \hat{H}_0(H, M)$ *provient de*

$$N'_{G/M} = \left(\sum_{g \in G/H} g^{-1} \right) : M_G \longrightarrow M_H$$
$$m \longmapsto \sum_{g \in G/H} g^{-1} m.$$

2. $Cor : \hat{H}^0(H, M) \to \hat{H}^0(G, M)$ *est induit par*

$$N_{G/H} = \left(\sum_{g \in G/H} g \right) : M^G \longrightarrow M^H$$
$$m \longmapsto \sum_{g \in G/H} gm.$$

Démonstration. Montrons 1. : Rappelons qu'on a

$$0 \longrightarrow M \otimes I_G \longrightarrow M \otimes \mathbb{Z}[G] \longrightarrow M \longrightarrow 0. \qquad (exacte)$$

On a $\delta : \hat{H}^0(G, M) \to \hat{H}^1(G, M \otimes I_G)$. De plus $Res : H^0(G, M) \to H^0(H, M)$ et $M^G \hookrightarrow M^H$ et est compatible avec δ, elle donne

$$Res : \hat{H}^0(G, M) \longrightarrow \hat{H}^0(H, M).$$

Par ailleurs, considérons $N'_{G/H} : \hat{H}^0(G, M) \to \hat{H}^0(H, M)$. Il faut vérifier la commutativité de

$$\begin{array}{ccc} \hat{H}^0(G, M) & \xrightarrow{\delta} & \hat{H}^0(G, M \otimes I_G) \\ \downarrow{\scriptstyle v = N_{G/H}} & & \downarrow{\scriptstyle Res} \\ \hat{H}^0(H, M) & \xrightarrow{\delta} & \hat{H}^0(H, M \otimes I_H) \end{array}$$

Soit $m \in M \otimes I_G$ qui reprovient $\bar{m} \in \hat{H}^0(G, M)$. On a $N_G(m) = 0$. Soit $m' \in M \otimes \mathbb{Z}[G]$ d'image m dans M. On a $N_G(m') = 0$ dans M et donc $m' \in (M \otimes \mathbb{Z}[G])^G$ et $m \in (M \otimes I_G)^G \subset (M \otimes I_G)^M$. Alors $N_G(m')$ modulo $N_H(M \otimes I_G)$ est $Res(\delta(\bar{m}))$. Par ailleurs, $v(\bar{m}) \equiv N'_{G/H}(m)$ modulo $I_H N$. De plus $\hat{\delta}(v(\bar{m}))$ est la classe de $N_H \circ N_{G/H}(m) = N_G(m)$.

On montre 2. de même. □

Proposition 3.13.5. *Considérons la composée*

$$\hat{H}^i(G,M) \xrightarrow{Res} \hat{H}^i(H,M) \xrightarrow{Cor} \hat{H}^i(G,M)$$

(pour $i \in \mathbb{Z}$). C'est la multiplication par $|G/H|$.

$$Cor \circ Res(x) = |G/H|x.$$

Démonstration. C'est vrai pour $i = 0$, d'après la Prop précédente, car $N_{G/H} \circ N'_{G/H} = |G/H|$. On déduit le cas $i \neq 0$ par décalage. □

Corollaire 3.13.6. *On a $|G| \cdot \hat{H}^i(G,M) = 0$ (l'exposant de $\hat{H}^i(G,M)$ divise $|G|$). Mais attention : ce n'est pas vrai en général pour $H^0(G,M)$ et $H_0(G,M)$.*

Démonstration. On considère $H = \{1\}$ et

$$\begin{array}{ccc} \hat{H}^i(G,M) & \xrightarrow{\times|G|} & \hat{H}^i(G,M) \\ & {\scriptstyle Res}\searrow \quad \nearrow{\scriptstyle Cor} & \\ & \hat{H}^i(\{1\},M) & \end{array}$$

□

Corollaire 3.13.7. *M est un $G-$module de type fini. $\hat{H}^i(G,M)$ est un groupe fini pour tout $i \in \mathbb{Z}$. Mais attention (encore) : ce n'est pas vrai en général pour $H^0(G,M)$ et $H_0(G,M)$.*

3.14 Cohomologie des groupes cycliques

Soit G un groupe fini cyclique d'ordre $|G| = m$. Soit g_0 un générateur de G. On a $N_G = \sum_{i=0}^{m-1}[g_0^i]$ et $I_G = \mathbb{Z}[G]([g_0]-[1])$. Posons pour $i \in \mathbb{Z}$, $K_i = \mathbb{Z}[G]$. Considérons

$$\begin{aligned} d : K_{i+1} &\longrightarrow K_i \\ x &\longmapsto ([g_0]-[1])x \qquad si\ i\ pair \\ x &\longmapsto N_G x \qquad si\ i\ impair. \end{aligned}$$

On a $\ker([g_0]-[1]) = \mathbb{Z}[G]^G = \operatorname{Im} N_G$ et $\operatorname{Im}([g_0]-[1]) = I_G = \ker N_G$. D'où la suite exacte

$$\cdots \longrightarrow \mathbb{Z}[G] \xrightarrow{[g_0]-[1]} \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{[g_0]-[1]} \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \longrightarrow \cdots$$

Soit M un $G-$module. On peut considérer le complexe $Hom(K, M)$. D'où

$$\hat{H}^i(G,M) = \begin{cases} \hat{H}^0(G,M) = {}^{M^G}\!/_{N_G M} & \textit{si } i \textit{ pair} \\ \hat{H}_0(G,M) = \ker N_G = {}^{M[N_G]}\!/_{I_G M} & \textit{si } i \textit{ impair.} \end{cases}.$$

Proposition 3.14.1. *On a* $H^2(G,\mathbb{Z}) \simeq {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ *(où* $n = |G|$*).*

Démonstration. On a $\hat{H}^0(G,\mathbb{Z}) = \hat{H}^2(G,\mathbb{Z}) = H^2(G,\mathbb{Z})$, or $\hat{H}^0(G,\mathbb{Z}) = {}^{\mathbb{Z}^G}\!/_{N_G\mathbb{Z}} = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. □

Soit G un groupe cyclique (fini). Soit M un $G-$module. On pose $h_i(G,M) = |\hat{H}^i(G,M)|$ ne dépend que la parité de $i \in \mathbb{Z}$. Si $h_0(G,M)$ et $h_1(G,M)$ sont finis, on pose

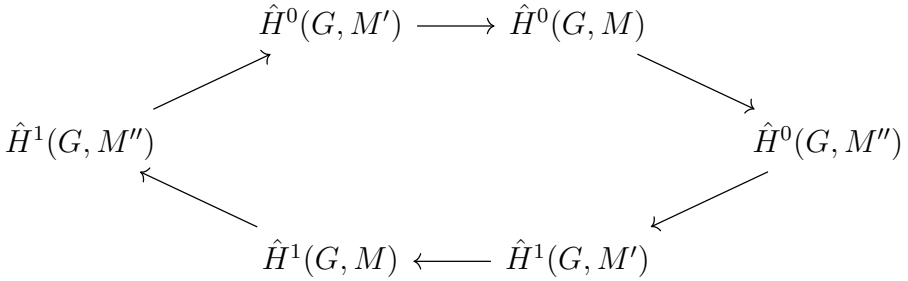
$$h(M) = {}^{h_0(M)}\!\Big/_{h_1(M)}\,.$$

C'est le quotient de Herbrand.

Proposition 3.14.2. *Soit* $0 \to M' \to M \to M'' \to 0$ *une suite exacte de* $G-$*modules. Si deux parmi* $h(M')$*,* $h(M)$*,* $h(M'')$ *sont définis, alors le troisième est défini et on a*

$$h(M) = h(M')h(M'').$$

Démonstration. Supposons que $\hat{H}^0(G,M)$, $\hat{H}^1(G,M)$, $\hat{H}^0(G,M')$, $\hat{H}^1(G,M')$ sont finis (on traite les autres cas de même) (i.e. $h(M')$ et $h(M)$ sont définis). On a la suite exacte longue, en fait un hexagone



Il faut montrer que $\hat{H}^0(G,M'')$ et $\hat{H}^1(G,M'')$ sont finis. Examinons l'exactitude en $\hat{H}^0(G,M'')$. On a

$$0 \longrightarrow X \longrightarrow \hat{H}^0(G,M'') \longrightarrow Y \longrightarrow 0$$

où X =image de $\hat{H}^0(G,M)$ qui est fini, et $Y \subset \hat{H}^i(G,M')$, qui est fini. Donc X et Y sont finis. Donc $\hat{H}^0(G,M'')$ est fini. Même argument pour $\hat{H}^1(G,M'')$, donc $h(G,M'')$ est défini. Tous les groupes de l'hexagone sont fini. Donc, comme la suite est exacte, on a

$$\frac{|\hat{H}^0(G,M')|}{|\hat{H}^0(G,M)|} \cdot \frac{|\hat{H}^0(G,M'')|}{|\hat{H}^0(G,M')|} \cdot \frac{|\hat{H}^0(G,M)|}{|\hat{H}^0(G,M'')|} = 1$$

(produit alterné des coordinate). Donc $h(M) = h(M')h(M'')$. □

Proposition 3.14.3. *Si M est un $G-$module fini, on a $h(G,M) = 1$.*

Démonstration. On a la suite exacte

$$\begin{aligned} 0 \longrightarrow M^G \longrightarrow M &\longrightarrow M \longrightarrow M_G \longrightarrow 0 \\ m &\longmapsto g_0 m - m \end{aligned}$$

où g_0 engendre G. On a donc $\frac{|M^G|}{|M|}\frac{|M|}{|M_G|} = 1$, donc $|M^G| = |M_G|$.

On a la suite exacte

$$0 \longrightarrow \hat{H}^1(G,M) \longrightarrow M_G \xrightarrow{N_G} M^G \longrightarrow \hat{H}^0(G,M) \longrightarrow 0.$$

On a

$$\frac{|\hat{H}^1(G,M)|}{\cancel{|M_G|}} \times \frac{\cancel{|M^G|}}{|\hat{H}^0(G,M)|} = 1.$$

Donc $|\hat{H}^1(G,M)| = |\hat{H}^0(G,M)|$. Donc $h(M) = 1$.

□

Corollaire 3.14.4. *Soit $f : M \to N$ un morphisme de $G-$ modules de noyau et conoyau finis. Si $h(M)$ est défini, alors $h(N)$ aussi et $h(M) = h(N)$. Réciproquement, si $h(N)$ est défini, alors $h(M)$ aussi et $h(N) = h(M)$.*

Démonstration. Si $h(M)$ est défini. On a les suites exactes

$$0 \longrightarrow \ker f \longrightarrow M \longrightarrow \operatorname{Im} f \longrightarrow 0$$

et

$$0 \longrightarrow \mathrm{Im}\, f \longrightarrow N \longrightarrow \mathrm{coker}\, f \longrightarrow 0.$$

On a $h(M) = h(\mathrm{Im}\, f)h(\ker f) = h(\mathrm{Im}\, f)$ et $h(\mathrm{Im}\, f)h(\mathrm{coker}\, f) = h(N)$, ou $h(\mathrm{coker}) = 1$. Donc $h(N) = h(\mathrm{Im}\, f) = h(M)$. □

3.15 Cohomologie galoisienne

Soit K un corps. Soit ${}^{L}/_{K}$ une extension galoisienne finie de K. On pose $G = Gal(L/K)$ groupe de Galois de l'extension ${}^{L}/_{K}$.

Premiers exemples de $G-$modules :
- $(L, +)$ pour $\sigma \in G$ et $x, y \in L$ on a $\sigma(x + y) = \sigma(x) + \sigma(y)$. On dit que $(L, +)$ est le $G-$module additif.

- $(L^{\times}, \times)$ pour $\gamma \in G$ et $x, y \in L^{\times}$. On a $\sigma(xy) = \sigma(x)\sigma(y)$. On dit que $(L^{\times}, \times)$ est le $G-$module multiplicatif.

- Soit n un entier≥ 1. On pose $\mu_n(L) = \{x \in L^{\times} \mid x^n = 1\}$. C'est un sous-$G-$module de $L^{\times}$.

Proposition 3.15.1. *On a $H^0(G, L) = K$, $H^0(G, L^{\times}) = K^{\times}$ et $H^0(G, \mu_n(L)) = \mu_n(K)$.*

Démonstration. On a

$$H^0(G, L) = L^G = \{x \in L \mid \sigma(x) = x \text{ pour tout } \sigma \in G\} = K.$$

Même argument pour les entres égalité. □

Proposition 3.15.2. *Soit $i \in \mathbb{Z}$. On a $\hat{H}^i(G, L) = 0$.*

Démonstration. On utilise le théorème de la base normale : il existe $x \in L$ tel que $((\sigma)(x))_{\sigma \in G}$ est une base de L comme $V-$espace vectoriel. (voir démonstration ci-après)

Alors

$$\begin{aligned} \mathbb{Z}[G] \otimes K &\simeq L \\ [\sigma] \otimes \lambda &\mapsto \lambda\sigma(x) \end{aligned}$$

Donc L est un module induit. Donc $\hat{H}^i(G, L) = 0$ pour tout i. □

Théorème 3.15.3. *(Hilbert 90) On a* $\hat{H}^1(G, L^\times) = H^1(G, L^\times) = 0$.

Démonstration. Soit $f : \sigma \mapsto a_\sigma$ un 1-cocycle dans $Z^1(G, L^\times)$. Pour $\sigma \in G$, $\substack{\sigma: L^\times \to L^\times \\ x \mapsto \sigma(x)}$ est multiplicative. C'est un caractère de G. On utilise l'indépendance linéaire des caractères : soit $(\lambda_\sigma)_{\sigma \in G}$ une famille d'élément de L tels que $\sum_{\sigma \in G} \lambda_\sigma \sigma(y) = 0$ pour tout y, alors $(\lambda_\sigma)_{\sigma \in G} = 0$.

Donc si $\sigma \mapsto a_\sigma$ est non nulle, il existe $c \in L^\times$ tel que $b = \sum_{\sigma \in G} a_\sigma \sigma(c) \neq 0$. Soit $\tau \in G$, on a

$$\begin{aligned} \tau(b) &= \sum_{\sigma \in G} \tau(a_\sigma) \tau\sigma(c) \\ &= \sum_{\tau \in G} a_\tau^{-1} a_{\tau\sigma} \tau\sigma(c) \\ &= a_\tau^{-1} b \end{aligned}$$

car $a_{\tau\sigma} = \tau(a_\sigma) a_\tau$ ($\sigma \mapsto a_\sigma$ est un $1-$cocycle). Donc $a_\tau = \frac{\tau(b^{-1})}{b^{-1}}$ est un $1-$cobord. Donc $H^1(G, L^\times) = 0$. □

Corollaire 3.15.4. *On a l'isomorphisme*

$$H^1(G, \mu_n(L)) = \hat{H}^1(G, \mu_n(L)) \simeq {}^{K^\times}\!/_{K^{\times n}}$$

où $K^{\times n}$ *=image de* $\substack{K^\times \to L^\times \\ x \mapsto x^n}$.

Démonstration. On a la suite exacte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_n(L) & \longrightarrow & L^\times & \longrightarrow & L^{\times n} & \longrightarrow & 0 \\ & & & & x & \longmapsto & x^n & & \end{array}$$

On a la suite exacte longue

$$0 \longrightarrow H^0(G, \mu_n(L)) \longrightarrow H^0(G, L) \longrightarrow H^0(G, L^{\times n}) \longrightarrow H^1(G, \mu_n(L)) \longrightarrow \underset{\| \\ 0}{H^1(G, L^\times)}.$$

On en déduit l'isomorphisme cherché. □

Cet énoncé est la théorie de Kummer. Lorsque L est algébriquement clos (donc $L^{\times n} = L^\times$) et G infini.

Théorème 3.15.5. *(indépendance linéaire des caractères) Soit H un groupe. Un caractère de K à valeurs dans K est un morphisme de groupes $H \longrightarrow K^\times$. Soient $\chi_1, \chi_2, \cdots, \chi_n$ des caractères de H à valeurs dans K. Alors $\chi_1, \chi_2, \cdots, \chi_n$ sont $K-$linéairement indépendants.*

Démonstration. Soient $a_1, a_2, \cdots, a_n \in K$ tels que $a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0$. On peut supposer que $a_1, \cdots, a_n \neq 0$ et que n est minimal.

Il existe $h \in H$ tel que $\chi_n(h) \neq \chi_{n-1}(h)$ car $\chi_n \neq \chi_{n-1}$. Pour $g \in G$, on a

$$\sum_{i=1}^{n} a_i\chi_i(gh) = 0 \qquad \textit{et de plus} \qquad \chi_n(h)\sum_{i=1}^{n} a_i\chi_i(g) = 0.$$

Donc $\sum_{i=1}^{n} a_i(\chi_i(h)\chi_i(g) - \chi_n(h)\chi_i(g)) = 0$. Donc $\sum_{i=1}^{n-1} a_i(\chi_i(h) - \chi_n(h))\chi_i(g) = 0$. Donc, comme n est minimal, et qu'on a

$$\sum_{i=1}^{n-1} a_i(\chi_i(h) - \chi_b(h))\chi_i = 0.$$

On a $a_i(\chi_i(h) - \chi_n(h)) = 0$ pour tout i. Donc $a_{n-1}(\underbrace{\chi_{n-1}(h) - \chi_n(h)}_{\neq 0}) = 0$. Donc $a_{n-1} = 0$. Absurde. D'où l'indépendence linéaire. □

Théorème 3.15.6. *Avec les hypothèses ci-dessus pour L, K, G. Il existe $x \in L$ tel que $(\sigma(x))_{\sigma\in G}$ est une base du $K-$espace vectoriel L.*

Démonstration. 1er cas : supposons K et L infini. Posons $L = K(x)$, avec $\alpha \in L$ primitif. Notons P le polynôme minimal de α. On a $d^\circ P = n = [L : K] = |G|$. Posons $\alpha_\sigma = \sigma(\alpha)$ pour $\sigma \in G$. On a $\alpha_1 = \alpha$. On a $\sigma(\alpha) \neq \sigma'(\alpha)$ si $\sigma \neq \sigma'$. Posons

$$\begin{aligned} Q_\sigma(x) &= \frac{P(x)}{(x - \alpha_\sigma)P'(\alpha_\sigma)} \\ &= \frac{\prod_{\tau\in G}(X - \alpha_\tau)}{(X - \alpha_\sigma)P'(\alpha_\sigma)} \end{aligned}$$

Si $\tau \neq \sigma$, on a $Q_\sigma(\alpha_\tau) = 0$. Si $\tau = \sigma$, on a $Q_\sigma(\alpha_\tau) = 1$. Posons $M(X) = (m_{\sigma,\tau}) \in M_{G\times G}(L[X])$ où $m_{\sigma,\tau} = \sigma\tau Q_1(X) = \sigma Q_\tau(X)$.

On a $M(\alpha) = (m_{\sigma,\tau}(\alpha))$ et

$$m_{\sigma,\tau}(\alpha) = \sigma Q_\tau(\alpha) = Q_{\sigma\tau}(\alpha) = \begin{cases} 0 & si\ \sigma\tau \neq 1 \\ 1 & si\ \sigma\tau = 1. \end{cases}$$

$M(\alpha)$ =matrice de permutation de G pour $\sigma \to \sigma^{-1}$. Posons $D(X) = \det M(X)$, on a $D(\alpha) = \underbrace{\det(M(\alpha))}_{permutation} \in \{-1, 1\}$. Donc $D(X) \neq 0$. Comme K est infini, il existe $a \in K$ tel que $D(u) \neq 0$. Posons $P = Q(a)$ et pour $\sigma \in G$, $\beta_\sigma = Q_\sigma(a) = \sigma(\beta)$ où $a \in K$.

Montrons que β convient. Supposons que $\sum_{\sigma\in G} \lambda_\sigma \sigma(\beta) = 0$ avec $\lambda_\sigma \in K$. On a pour $\sigma \in G$, $\tau\left(\sum_{\sigma\in G} \lambda_\sigma \sigma(\beta)\right) = 0$, et donc $\sum_\sigma \lambda_\sigma \tau\sigma(\beta) = 0$. Donc $M(a)\times$vecteur$(\lambda_\sigma)_{\sigma\in G} = 0$. Mais $M(a)$ inversible. Donc $(\lambda_\tau)_{\tau\in G} = 0$. Cela achève le cas où K est infini.

$\underline{2^{eme}\ \text{cas}}$: le corps K est fini. Posons $K = \mathbb{F}_q$, corps à q éléments et $L = \mathbb{F}_{q^n}$ avec $n = |G| = [L : K]$. Notons

$$\begin{aligned} \varphi : L &\longrightarrow L \\ x &\longmapsto x^q \end{aligned}$$

la Frobenius $\in G$. On a $G = \{1, \varphi, \varphi^2, \cdots, \varphi^{n-1}\}$. φ est $K-$linéaire. On a $\varphi^n = 1$. Le polynôme minimal de φ est $X^n - 1$. Donc L est un $K[X]-$module par

$$\begin{aligned} K[X] \times L &\longrightarrow L \\ (P, X) &\longmapsto P(\varphi)(x). \end{aligned}$$

Comme L est fini, il est de type fini comme $K[X]-$module. Comme $K[X]$ est principal, il existe $P_1, P_2, \cdots, P_k \in K[X]$ tels que

$$L \simeq \prod_{i=1}^{k} K[X]\Big/(P_i)$$

avec $P_i = 0$ impossible, et alors ce qui est unitaire car L fini, avec $P_{i+1}|P_i$.

Alors le polynôme minimal de φ est $ppcm(P_1, \cdots, P_k) = P_1 = X^n - 1$. De plus

$$\begin{aligned}\dim_K L &= \sum_{i=1}^{k} \dim \left(K[X] \Big/ (P_i) \right) \\ &= \sum_{i=1}^{k} d^\circ(P_i).\end{aligned}$$

Or

$$d^\circ P_1 = n = [L : K] = \dim_K L = d^\circ P_1 + \sum_{i=2}^{k} d^\circ P_i.$$

Donc $k = 1$ et $P_1 = X^n - 1$ et $L \simeq {K[X]}/{X^n - 1}$ (comme $K-$espace vectoriel). Notons $\alpha \in L$ l'image de 1. Comme $1, X, \cdots, X^{n-1}$ est une base de ${K[X]}/{X^n - 1}$. $\alpha, \varphi(\alpha), \cdots, \varphi^{n-1}(\alpha)$ est une base de L comme $K-$espace vectoriel. □

Revenons à la cohomologie galoisienne. On pose $B_r(L/K) = H^2(G, L^\times)$. C'est le groupe de Brauer relatif à l'extension ${L}/{K}$.

Proposition 3.15.7. *Supposons que $L^{\times n} = L^\times$. On a l'isomorphisme $B_r(K)[n] = \{x \in B_r(K) \mid nx = 0\} \simeq H^2(G, \mu_n(L))$.*

Démonstration. On a la suite exacte

$$\begin{aligned}1 \longrightarrow \mu_n(L) \longrightarrow L^\times &\longrightarrow L^\times \longrightarrow 0 \\ x &\longmapsto x^n\end{aligned}$$

d'où

$$\longrightarrow \underbrace{H^1(G, L^\times)}_{\| \ 0} \longrightarrow H^2(G, \mu_n(K)) \longrightarrow H^2(G, L^\times) \longrightarrow H^2(G, L^\times) \longrightarrow$$

cela donne l'isomorphisme. □

En générale, B_r est difficile à calculer. Il dépend de K.

Proposition 3.15.8. *$K = \mathbb{R}$, $L = \mathbb{C}$, on a $B_r(L/K) \simeq {\mathbb{Z}}/{2\mathbb{Z}}$.*

Démonstration. On a $G = \{1, \textit{conjugaison complexe}\}$. Donc G est cyclique d'ordre 2. On a $H^2(G, \mathbb{C}^\times) = \hat{H}^0(G, \mathbb{C}^\times) = {\mathbb{C}^{\times G}}\Big/{N_G(\mathbb{C}^\times)}$, $\mathbb{C}^{\times G} = \mathbb{R}$ et $N_G(z) = z \cdot \bar{z} = |z|^2$. Donc $N_G(\mathbb{C}^\times) = \mathbb{R}_+^\times$. Donc $H^2(G, \mathbb{C}^\times) \simeq {\mathbb{R}^\times}\Big/{\mathbb{R}_+^\times} \simeq {\mathbb{Z}}/{2\mathbb{Z}}$ □

Proposition 3.15.9. *Supposons K et L finies, on a $B_r(L/K) = \{0\}$.*

Démonstration. Posons $K = \mathbb{F}_q$, $L = \mathbb{F}_{q^n}$. C'est une extention cyclique. On a $H^2(G, L^\times) = \hat{H}^0(G, L^\times)$. Comme $L^\times$ est fini, on a $h(G, L^\times) = 1$. Donc $h_0(G, L^\times) = h_1(G, L^\times)$. Or $h_1(G, L^\times) = |H^1(G, L^\times)| = 1$ par *Hilbert* 90. Donc $\hat{H}^0(G, L^\times) = \{0\}$. Donc $H^2(G, L^\times) = \{0\}$. □

Remarques 3.15.10. *Pour $K = \mathbb{Q}$ et extension fini de K, le calcul est difficile. Pour $K = \mathbb{Q}_p$ (corps des nombres p-adique), c'est plus facile. On montre que $B_r(L/K)$ est fini et contenu dans $\mathbb{Q}/\mathbb{Z}$ (il est donc cyclique).*