Schéma affine en groupe

Langlois Kévin

Eté 2008

“ J’etais en proie à la mathématique,
Temps sombre! enfant ému du frisson poétique,
Pauvre oiseau qui heurtais du crâne mes barreaux,
On me livrait tout vif aux chiffres, noirs bourreaux ;
On me faisait de force ingurgiter l’algèbre ; ”

Victor Hugo (Besançon 1802 - Paris 1885) , Contemplations (1856).

Nous rappelons quelques faits d'algèbre commutative qui nous servirons par la suite. Tout nos anneaux seront commutatifs unifères. Par une extension de corps L/K on entend la donnée d'un morphisme de K vers L. L est alors une algébre sur le corps K et on dit que l'algébre L est de type finie s'il existe des éléments $x_1, x_2, ..., x_n \in L$ tel que $K[x_1, x_2, ..., x_n] = L$. Le résultat suivant est dû à Samuel Zariski.

Proposition 1 *Toute extension de corps de type fini en tant qu'algébre est de dimension finie.*

Démonstration Notons L/K une extension de corps satifaisant les hypothèses du théorème. Donc il existe des éléments $x_1, x_2, ..., x_N$ de L tels que $L = K[x_1, x_2, ..., x_N]$. Montrons le résultat par récurrence sur l'entier N. Puisque $K(x_1) = K[x_1]$ équivaut à x_1 algébrique sur K, on déduit le cas $N = 1$. Supposons le résultat vrai pour N fixé. Donc sous cet hypothèse : $L = K[x_1, x_2, ..., x_{N+1}]$. Si x_{N+1} est un nombre algébrique sur K, alors on applique l'hypothèse de récurrence à la formule :

$$[L : K] = [K(x_{N+1})[x_1, x_2, ..., x_N] : K(x_{N+1})][K(x_{N+1}) : K]$$

Si x_{N+1} n'est pas un nombre algébrique alors ceci n'est pas possible. En effet, soit $i = 1, ..., N$, il existe un polynôme P_i à coefficient dans $K(x_{N+1})$ tel que $P_i(x_i) = 0$. Notons a_i un élément non nul de $K[x_i]$ tel que le produit de tout coefficient de P_i par celui-ci soit dans $K[x_{N+1}]$, a le produit de tous les a_i et y un élément de $K(x_{N+1})$. Donc il existe un entier $p \geq 1$, tel que ya^p soit un entier algébrique sur $K[x_{N+1}]$. Or $K[x_{N+1}]$ est isomorphe en tant qu'anneau aux polynômes $K[X]$ à une variable X, donc $K[x_{N+1}]$ est intégralement clos. Donc si $y = 1/b$ avec b un élément de $K[x_{N+1}]$ premier avec a alors $a^p/b \in K[x_{N+1}]$, ce qui est une contradiction.

Définition Soit R un anneau et $\mathfrak{a}$ un idéal de R. On appelle racine de $\mathfrak{a}$ que l'on note $\sqrt{a}$, l'ensemble des éléments b de R tels qu'il existe un entier $N \geq 1$ tel que b^N. Par suite, on appelle idéal radical tout idéal égal à sa racine.

Nous laissons au lecteur le soin de vérifier que $\sqrt{a}$ est un idéal de R.

Lemme 1 *Soit R un anneau. Si S est une partie multiplicative ne contenant pas 0 alors il existe un idéal premier $\mathfrak{p}$ tel que $\mathfrak{p} \cap S = \emptyset$.*

Démonstration Soit X l'ensemble des idéaux $\mathfrak{a}$ tels que $S \cap \mathfrak{a} = \emptyset$. X est non vide car il contient l'idéal nul et est inductif pour l'inclusion. Donc par le lemme de Zorn, X possède un élément maximal $\mathfrak{p}$. Il reste à montrer que $\mathfrak{p}$ est premier. Soient a, b deux éléments de R n'appartenant pas à $\mathfrak{p}$ tels que $ab \in \mathfrak{p}$. Donc il existe $s_1, s_2 \in S$ tels que $s_1 \in (a, \mathfrak{p})$ et $s_2 \in (b, \mathfrak{p})$. Or en ecrivant s_1 et s_2 comme combinaisons linéaires sur R de a, b et d'éléments de $\mathfrak{p}$, on observe que $s_1 s_2 \in \mathfrak{p}$, ce qui est absurde. D'où le résultat.

Proposition 2 *Soit R un anneau et $\mathfrak{a}$ un idéal de R alors la racine de $\mathfrak{a}$ est exactement l'intersection de tous les idéaux premiers de R contenant $\mathfrak{a}$.*

Démonstration En passant aux quotients, on est amené à montrer qu'un élément est nilpotent si seulement si il appartient à tout idéal premier de R. Si a n'est pas nilpotent alors par le lemme précédent la partie mutiplicative des puissances positives de a est dijointe d'un idéal premier. La réciproque se déduit par définition d'un idéal premier.

Soient K un corps algébrique clos,

$$X = (X_1, X_2, ..., X_n)$$

un système d'indéterminées et P un polynôme de $K[X]$. Un élément $a \in K^n$ est un zéro de P si $P(a) = 0$.

Définition Soit S une partie de $K[X]$, on note $Z(S)$ les zéros communs aux éléments de S. Un partie $Y \subset K^n$ est algébrique s'il existe une partie $S' \subset K[X]$ telle que $Y = Z(S')$. Si T est un sous-ensemble de K^n alors on note $I(T)$ l'idéal des polynômes s'annulant sur T, nous l'appelons l'idéal associé à T.

L'assertion suivante est le théorème des zéros (Nullstellensatz) de Hilbert.

Théorème 1 *Les idéaux maximaux de $K[X]$ sont exactement les idéaux de la forme*

$$(X_1 - a_1, X_2 - a_2, ..., X_n - a_n)$$

En particulier, si $\mathfrak{a}$ est un idéal de $K[X]$ alors

$$I \circ Z(\mathfrak{a}) = \sqrt{a}$$

Démonstration Soit $\mathfrak{a}$ un idéal maximal de $K[X]$ et notons $L = K[X]/\mathfrak{a}$. Puisque $K[X]$ est noethérien, l'extension L/K est de type finie. Donc L/K est finie par une proposition précédente. En outre, K est algébriquement clos et tout élément de L est algébrique sur K. Donc $K = L$. On a donc une suite de morphismes naturels :

$$K[X] \longrightarrow K[X]/\mathfrak{a} \longrightarrow K$$

Notons a_i l'image X_i par cette composition. Donc l'idéal propre $(X_1 - a_1, ..., X_n - a_n)$ contient $\mathfrak{a}$. D'où la première affirmation. Montrons la deuxième. Soient $f \in I \circ Z(\mathfrak{a})$ et $P_1, P_2, ..., P_N$ des polynômes tels que $\mathfrak{a} = (P_1, P_2, ..., P_N)$. Nous allons utiliser l'astuce de Rabinovitsch. Notons par le fait précédent et le théorème de Krull que $Z(\mathfrak{a})$ est vide si et seulement si $1 \in \mathfrak{a}$. Donc l'idéal de

$K[X,Y]$ (avec Y une indéterminée) engendré par $P_1, ..., P_N, 1 - YP$ contient 1. Donc il existe des polynômes $Q_0, Q_1, ..., Q_N$ tels que

$$1 = P_0(X)(1 - YP(X)) + Q_1(X,Y)P_1(X) + ... + Q_N(X,Y)P_N(X)$$

Ensuite en remplaçant Y par $1/P$ et en éliminant les dénominateurs par la multiplication de P^s pour s un entier strictement positif assez grand, il vient : $P^s \in \mathfrak{a}$. Donc $I \circ Z(\mathfrak{a}) \subset \sqrt{a}$. Enfin l'inclusion inverse se déduit des définitions de I et Z.

Contents

1 Introduction

1.1 Schéma

1.1.1 Schéma affine associé à une variété algébrique

Soit n un entier ≥ 1.

Le but de ce paragraphe est de donner une intuition géométrique de la notion de schéma affine. Soit $X = (X_1, ..., X_n)$ un système à n indéterminées. Nous notons pour l'instant $R = K[X]$ l'anneaux des polynômes à plusieurs variables sur un corps K algébriquement clos. Du préliminaire d'algébre précédent, on en tire des résultats de géométrie :

Proposition 3 *L'application Z définit une application bijective de l'ensemble des idéaux radicaux vers les ensembles algébriques de K^n. En particulier, la restriction de Z aux idéaux maximaux est une bijection avec K^n.*

Démonstration Tout d'abord l'ensemble des idéaux radicaux est non vide car il contient toutes les racines de tous les idéaux. Soit $\mathfrak{a}$ un idéal radical de $K[X]$. Donc :

$$I \circ Z(\mathfrak{a}) = \sqrt{\mathfrak{a}} = \mathfrak{a}$$

Si Y est un ensemble algébrique alors :

$$Z \circ I(Y) = Y$$

D'où la première assertion. Montrons la deuxième. A nouveau par le théorème des zéros de Hilbert, l'application

$$(X_1 - a_1, ..., X_n - a_n) \longmapsto (a_1, ..., a_n)$$

est une bijection.

Notons que l'application Z renverse les inclusions, en ce sens que si $I_1 \subset I_2$ sont deux idéaux alors $Z(I_2) \subset Z(I_1)$.

Définition On appelle fermé de Zariski dans K^n tout ensemble algébrique de K^n. Les fermés de Zariski forment une topologie sur K^n dite topologie de Zariski.

Définition Un ensemble algébrique Y de K^n est une variété algébrique si son idéal associé est premier. En outre, on dit que T est une sous-variété de Y si T est une variété de K^n incluse dans Z.

Ainsi une variété Y est solution d'un système polynômial :

$$P_1(X) = P_2(X) = ... = P_N(X) = 0$$

où $P_1, ..., P_N$ engendre un idéal premier. Puisqu'un idéal premier est égal à sa racine, il s'ensuit que la correspondance entre varitétés algébriques de K^n et idéaux premiers associés à celles-ci est bijective. Par ailleurs, l'etude des ensembles algébriques est réduite à celle des variétés :

Proposition 4 *Tout ensemble algébrique sur un corps algébriquement clos s'écrit comme union finie de variétés déterminées de manière unique.*

Démonstration

Soit Y une variété de K^n.

Définition Si Y est associée à un idéal premier $\mathfrak{p}$ alors on note $\mathcal{O}_Y$ l'anneau $R/\mathfrak{p}$ dit des fonctions régulières sur Y.

Des remarques précédentes, il s'ensuit :

Proposition 5 *L'ensemble des idéaux premiers $Spec(\mathcal{O}_Y)$ de $\mathcal{O}_Y$, dit spectre de $\mathcal{O}_Y$, est en bijection avec l'ensemble des sous-variétés de Y. En particulier, les points de Y s'identifie avec les idéaux maximaux de $\mathcal{O}_Y$.*

Définition Soit S un sous-ensemble de $\mathcal{O}_Y$, on note $V(S)$ l'ensemble des idéaux premiers contenant S. On appelle topologie spectrale sur $Spec(\mathcal{O}_Y)$ la topologie dont les fermés sont de la forme $V(S)$. Par suite, $Spec(\mathcal{O}_Y)$ muni de la topologie spectrale est appelé schéma affine associé à la variété Y.

La proposition suivante montre la proximité entre topologie de Zariski et topologie spectrale :

Proposition 6 *Si l'on identifie $Specm(\mathcal{O}_Y)$ avec l'ensemble des sous-variétés de Y alors la topologie de Zariski sur Y est la topologie spectrale induite par son schéma affine associé.*

Démonstration Soient F un fermé de Y et $\mathfrak{p} = I(Y)$. Donc il existe un idéal radical $\mathfrak{a}$ de $K[X]$ tel que $F = Z(\mathfrak{a})$. Il suffit de montrer que $Z(\mathfrak{a}) \cap V(\mathfrak{p}) = Z(\mathfrak{a})$. L'inclusion $Z(\mathfrak{a}) \cap V(\mathfrak{p}) \subset Z(\mathfrak{a})$ est toujours vraie. Soit p un point de $Z(\mathfrak{a})$, $\{p\}$ est associé à un idéal maximal $\mathfrak{m}$ contenant $\mathfrak{a}$ et appartient à $V(\mathfrak{a})$, d'où l'inclusion inverse.

Donnons quelques exemples :

Exemple 1: Composantes irreductibles D'après le théorème de transfert de Gauss que $K[X]$ est factoriel. Donc un élément de $K[X]$ est irreductible si et seulement si il engendre un idéal premier. De plus, si T est un ensemble algébrique $T = Z(P)$ alors on écrit :

$$P = \prod_{i=1}^{N} P_i^{\nu_i}$$

avec P_i des polynômes irreductibles. En appliquant Z

$$T = Z(\prod_{i=1}^{N} P_i^{\nu_i}) = \bigcup_{i=1}^{N} Z(P^{\nu_i}) = \bigcup_{i=1}^{N} Z(\sqrt{P_i^{\nu_i}}) = \bigcup_{i=1}^{N} Z(P_i)$$

et T a pour composantes irreductibles les $Z(P_i)$.

Exemple 2: Intersection de courbes Si P, Q sont deux polynômes non nuls, non inversibles de $K[X_1, X_2]$ et sans facteurs communs alors le système

$$P(X_1, X_2) = Q(X_1, X_2) = 0$$

n'a qu'un nombre fini de solutions. En effet, comme $K(X_1)[X_2]$ est principal il existe des éléments R, S de celui-ci tels que : $RP + SQ = 1$. Soit $D \in K[X_1]$ tels que $DRP, DSQ \in K[X_1, X_2]$. Donc si (x, y) est solution du système d'equation ci-dessus alors

$$DRP(x, y) + DSQ(x, y) = D(x) = 0$$

Il y a donc qu'un nombre fini de possibilités pour x. Enfin, on intervertit les variables X_1, X_2 dans les raisonnements précédents.

Exemple 3 : Courbe algébrique plane

(a) Si C est une courbe algébrique plane (i.e une variété de K^2 de dimension 1) alors $I(C)$ est engendré par un seul élément. En effet, notons $I(C) = (P_1, P_2, ..., P_N)$ avec $P_1, P_2, ..., P_N$ des polynômes non nuls de $K[X_1, X_2]$ tels que leurs facteurs irreductibles ne soient pas dans $I(C)$ (On peut toujours se ramener à ce cas). Or $I(C)$ est premier, donc chaque P_i est irreductitble. Supposons que $P_1, P_2, ..., P_N$ n'aient pas de facteurs communs alors par l'exemple précédent ceci est absurde. Donc $P_1, P_2, ..., P_N$ ont un facteur commun S que l'on peut à nouveau supposer irreductible et il vient : $I(C) = (S)$.

(b) Déterminons les sous-variétés de C. Soit T une sous-variété de C de dimension 1. Donc il existe un polynôme irredicutible U tel que $I(T) = (U)$. Donc $S = UP$ pour $P \in K[X_1, X_2]$. Donc par irreductibilité de S, $I(C) = I(T)$ et $T = C$.

(c) Si M est une sous-variété de C de cardinal fini alors M est un singleton. En effet, écrivons M comme union disjointe de singletons :

$$\{x_1\} \cup \{x_2\} ... \cup \{x_k\}$$

Donc :

$$I(M) = \bigcap_{i=1}^{k} I(\{x_i\})$$

Si $k > 1$, notons R_i un générateur de $I(\{x_i\})$. Donc le produit des R_i est élément de $I(M)$ mais chaque R_i n'appartient pas à $I(M)$. Ce qui contredit que $I(M)$ est premier. En résumé, on a déterminé entièrement le schéma affine $Spec(K[X_1, X_2]/I(C))$ qui est composé de points M et du point générique $I(C)$.

Exemple 4 : Plan affine On note $\mathbb{A}^2_K$ le schéma affine $Spec(K[X_1, X_2])$. Les points de $\mathbb{A}^2_K$ sont donc de trois types différents. Les singetons donnés par les idéaux maximaux de $K[X_1, X_2]$, les sous-variétés de dimension 1 données par une seule équation (voir l'exemple 3) et le point générique correspondant à l'idéal nul qui est dense partout.

Exemple 5 : Lemniscate Considérons l'ensemble algébrique L sur les complexes défini par l'equation :

$$P = Y^2 - X^2 + (X^2 + Y^2)^2 = 0$$

En fait, L est une courbe algébrique plane. (i.e une variété algébrique de dimension 1 sur le plan $\mathbb{C}^2$). Car en développant :

$$P = Z^2 + Z(2Y^2 - 1) + Y^2 + Y^4$$

avec le changement de variables $Z = X^2$. Supposons qu'il existe deux polynômes S_1, S_2 en les variables Z, Y tels que $S_1 S_2 = P$. Si les degrés de S_1, S_2 en Z sont strictement positifs alors il existe deux polynômes $P_1(Y), P_2(Y)$ tels que : $S_i = Z - P_i(Y)$ pour $i = 1, 2$. Donc en multipliant S_1 par S_2 et en identifiant, il s'ensuit :

$$P_1 + P_2 = -2Y^2 + 1$$

$$P_1 P_2 = Y^4 + Y^2$$

Et on obtient l'equation :

$$P_1^2 + P_1(2Y^2 - 1) + Y^4 + Y^2$$

que l'on met sous forme canonique :

$$(P_1 - Y^2 - \frac{1}{2})^2 = 2(Y - \frac{\sqrt{8}}{8})(Y + \frac{\sqrt{8}}{8})$$

Mais cette dernière equation contredit l'unicité de la décomposition en irréductibles dans $\mathbb{C}[Y]$. Par conséquent, le degré de l'un des S_i en Z est nul, disons S_1. Ensuite, on conclut en remarquant que $P(Z,Y)$ est unitaire et que le degré de S_1 en Y est forcément nul. En fait la courbe L sur les réels est appelée lemniscate. On peut montrer que sa longueur d'arc est donnée par l'intégrale elliptique :

$$z(r) = \int_0^r \frac{1}{\sqrt{1-r^4}}$$

dont l'inverse appelé sinus lemniscatique se prolonge en une fonction méromorphe de developpement en 0 :

$$z - \frac{1}{10}z^5 + \frac{1}{120}z^9 - \frac{11}{15600}z^{13} + ...$$

Exemple 6 : Cubique de Fermat On suppose que K est de caractérisque nul. Considérons la surface donnée par l'equation : $X_1^3 + X_2^3 + X_3^3$ et ζ une racine cubique non réelle de l'unité. De l'identité :

$$-X_3^3 = (X_1 + X_2)(X_1 + \zeta X_2)(X_1 + \zeta^2 X_2)$$

On déduit que $Spec(K[X_1, X_2, X_3]/(X_1^3 + X_2^3 + X_3^3)$ a des éléments associés à des variétés de dimension 1. En effet, l'idéal $\mathfrak{a}_s = (X_3, X_1 + \zeta^s X_2)$ avec s un entier est premier puisque l'on a la suite d'isomorphismes :

$$K[X_1, X_2, X_3]/\mathfrak{a}_s \longrightarrow K[X_1, X_2]/(X_1 + \zeta^s X_2] \longrightarrow K[X_2]$$

Ces morphismes étant donnés par la factorisation des morphismes surjectifs :

$$P(X_1, X_2, X_3) \longmapsto P(X_1, X_2, 0)$$

et :

$$P(X_1, X_2) \longmapsto P(-\zeta^s X_2, X_2)$$

1.1.2 Faisceaux d'anneaux

Nous allons définir la notion de schéma, pour cela nous faisons une disgression sur les faisceaux. On suppose que le lecteur est accoutumé au langage fonctoriel. Soit X un espace topologique. On note $\mathfrak{Top}(X)$ la catégorie dont les objets sont les ouverts de X et les morphismes sont les inclusions.

Définition On appelle préfaisceau d'anneaux sur X un foncteur contravariant $\mathcal{O}$ de la catégorie $\mathfrak{Top}(X)$ dans la catégorie des anneaux.

Ce qui signifie que pour tout ouvert $\mathfrak{V}$, on associe un anneau $\mathcal{O}(\mathfrak{V})$ et pour toute inclusion $i : U \longrightarrow V$ entre deux ouverts de X un morphisme d'anneaux $\rho_{V,U} = \mathcal{O}(i) : \mathcal{O}(V) \longrightarrow \mathcal{O}(U)$ dit restriction de V à U vérifiant la règle dite de cocycle :

$$\rho_{V,U} \circ \rho_{W,V} = \rho_{W,U}$$

pour toutes inclusions d'ouverts $U \subset V \subset W$. On convient que $\mathcal{O}(\emptyset) = \{0\}$.

Définition Un préfaisceau d'anneaux $\mathcal{O}$ sur X est un faisceau d'anneaux sur X si $\mathcal{O}$ vérifie l'axiome suivant dit des faisceaux :

(FAI 1) Si pour tout recouvement d'ouverts $\{\mho_\alpha\}_\alpha$ et si pour tous indices α, β il existe des sections $s_\alpha \in \mathcal{O}(U_\alpha)$ de $s_\beta \in \mathcal{O}(U_\beta)$ telles que leurs restrictions à $U_\alpha \cap U_\beta$ soient égales alors il existe une unique section globale $s \in \mathcal{O}(Z)$ telle que pour tout indice α la restriction de s à U_α soit égale à s_α.

L'anneau des sections globales doit être vu comme un "anneau de fonctions", l'axiome des faisceaux traduisant une propriété locale de ces fonctions. Donnons des exemples pour illustrer cette dernière remarque.

Exemple 1 : Distributions On considére $\mathbb{R}^n$ muni de sa topologie usuelle. Soit $\mho$ un ouvert de $\mathbb{R}^n$, on note $\mathcal{D}'(\mho)$ l'espace des distributions sur $\mho$. On observe que $\mathcal{D}'$ est un préfaisceau de modules sur $\mathcal{C}^\infty$. Ensuite, en faisant une partition de l'unité pour tout recouvement d'ouverts de $\mathbb{R}^n$, on déduit que $\mathcal{D}'$ vérifie l'axiome des faisceaux. Nous utiliserons cette dernière astuce pour définir la notion de schéma affine.

Exemple 2 : Variétés algébriques Soient T une variété algébrique de K^n et $\mho \subset T$ un ouvert. On note $\mathcal{O}(\mho)$ l'anneau des fonctions régulières sur $\mho$. Donc $f : \mho \longrightarrow K$ est régulière si pour tout point $y \in \mho$, il existe un voisinage ouvert W de y tel que $f|W$ soit une fraction rationnelle de $K(X)$ sans pôle sur W. On remarque que le caractère local de la régularité implique que $\mathcal{O}$ est un faisceau d'anneau sur T. On notera que $\mathcal{O}(T) = \mathcal{O}_T$.

Définition Soient $\mathcal{O}_1$,$\mathcal{O}_2$ deux faisceaux d'anneaux sur X. On appelle morphisme de faisceaux de $\mathcal{O}_1$ vers $\mathcal{O}_2$ une transformation naturelle de $\mathcal{O}_1$ vers $\mathcal{O}_2$.

De manière plus concrète, un morphisme $F : \mathcal{O}_1 \longrightarrow \mathcal{O}_2$ de faisceaux est la donnée pour toute inclusion $i : U \longrightarrow V$ d'ouverts d'un morphisme d'anneaux $F(U) : \mathcal{O}_1(U) \longrightarrow \mathcal{O}_2(U)$ tel que :

$$\mathcal{O}_2(i) \circ F(V) = F(U) \circ \mathcal{O}_1(i)$$

Exemple 3 : Morphisme de variétés algébriques Cette dernière définition nous permet de définir les morphismes entre variétés algébriques. Soient $(Y, \mathcal{O}_1)$, $(Z, \mathcal{O}_2)$ deux variétés algébriques munient de leurs faisceaux d'anneaux des fonctions régulières. Une application continue $\alpha : Y \longrightarrow Z$ est un morphisme de variétés algébriques si la composition de chaque section par α induit un morphisme de faisceaux de $\mathcal{O}_2$ vers $\alpha_*\mathcal{O}_1$. (où l'on note $\alpha_*\mathcal{O}_1$ le faisceau sur Z tel que pour tout ouvert $\mho$ de Z, $\alpha_*\mathcal{O}_1(\mho) = \mathcal{O}_1(\alpha^{-1}(\mho))$.) Par ailleurs, nous notons $\mathfrak{Var}(K)$ la catégorie des variétés algébriques sur le corps K.

Définition Soit $\mathcal{O}$ un faisceau d'anneaux sur X et x un point de X. On appelle anneaux des germes en x l'anneau $\mathcal{O}_x$ formé de classes d'equivalences $[U, f]$ de couples (U, f) avec U un ouvert contenant x et $f \in \mathcal{O}(U)$ une section de U où l'on identifie deux couples (U, f) et (V, g) s'il existe un voisinage ouvert W de x contenu dans $U \cap V$ tel que les restrictions de f et g sur W soient égales.

Si $x \in U$ alors on a un morphisme d'anneaux :

$$\mathcal{O}(U) \longrightarrow \mathcal{O}_x$$

qui à tout section $f \in \mathcal{O}(U)$ associe la classe $[U, f]$.

En fait, la notion de germe de fonctions est connue :

Exemple 4 : Fonctions holomorphes Considérons le faisceau $\mathcal{O}$ d'anneaux des fonctions holomorphes sur le plan complexe. Si z est un nombre complexe alors $\mathcal{O}_z$ est l'anneaux des classes de fonctions holomorphes au voisinage de z, où l'on identifie deux fonctions si elles sont égales sur un disque contenant z.

Donc intuitivement par une germe de fonctions en x, on entend une fonction ayant la propriété locale donnée par $\mathcal{O}$ seulement au voisinage de x.

Exemple 5 : Espace étalé Soit $\mathcal{O}$ un faisceau d'anneaux sur X. On considére l'union disjointe $\overline{\mathcal{O}}$ des $\mathcal{O}_x$ où $x \in x$. Sur $\overline{\mathcal{O}}$ on peut défnir une topologie de la manière suivante. Si l'on note s_x un élément de $\mathcal{O}_x$ représenté par une section s et $\mho$ un ouvert de x alors on considère la topologie engendré par les ouverts :

$$\mho(s) = \bigcup_{x \in \mho} s_x$$

On a ainsi la projection naturelle continue :

$$\pi : \overline{\mathcal{O}} \longrightarrow x$$

On peut montrer que les sections du faisceau $\mathcal{O}$ s'inditifient avec les applications s telles que $\pi \circ s$ soit identité, ce qui justifie la nomemclature section. Pour cela, il suffit de correspondre à une section s sur un ouvert $\mho$ l'application qui à tout $x \in \mho$ associe s_x.

Exemple 6 : Morphisme induit Si $F : \mathcal{O}_1 \longrightarrow \mathcal{O}_2$ est uN morphisme de faisceaux sur X alors pour tout $x \in X$, on a un morphisme naturel :

$$F_x : \mathcal{O}_{1,x} \longrightarrow \mathcal{O}_{2,x}$$

Proposition 7 *Soit $\mathcal{O}$ presfaisceau sur X. On note $\mathcal{O}'$ le presfaisceau dont une section s' est définie par l'application :*

$$s' : \mho \ni x \longmapsto [\mho, s] \in \mathcal{O}_x$$

pour $\mho$ un ouvert de X et $s \in \mathcal{O}(\mho)$. Alors $\mathcal{O}'$ est un faisceau sur X.

Démonstration Soient $\{\mathcal{U}_\alpha\}$ un recouvrement ouvert de X et $s \in \mathcal{O}'(X)$ une section globale telle que $s|\mathcal{U}_\alpha = 0$ pour tout α. Montrons que $s = 0$. Soit $x \in X$, il existe α tel que $x \in \mathcal{U}_\alpha$ et donc $s(x) = [\mathcal{U}_\alpha, s] = 0$. Maintenant, soit $\{s_\alpha\}$ une famille de sections telle que $s_\alpha|\mathcal{U}_\alpha \cap \mathcal{U}_\beta = s_\beta|\mathcal{U}_\alpha \cap \mathcal{U}_\beta$. pour tous α, β. Montrons qu'il existe s tel que $s|\mathcal{U}_\alpha = s_\alpha$ pour tout α. On définit alors s par :

$$s(x) = [\mathcal{U}_\alpha, s_\alpha]$$

si $x \in \mathcal{U}_\alpha$. s est bien définie par hypothèse sur $\{s_\alpha\}$ et vérifie ce que l'on veut. Enfin, s est déterminée de manière unique par ce qui précéde.

Soient $\mathcal{O}_1, \mathcal{O}_2$ deux faisceaux sur X. La proposition précédente nous donne les constructions algébriques suivantes :

Exemple 7 : Somme directe Soit X un espace topologique et $\mathcal{O}_1, \mathcal{O}_2$ deux faisceaux sur X. On note $\mathcal{O}_1 \oplus \mathcal{O}_2$ le presfaisceau sur X défini par

$$\mathcal{O}_1 \oplus \mathcal{O}_2(\mathcal{U}) = \mathcal{O}_1(\mathcal{U}) \oplus \mathcal{O}_2(\mathcal{U})$$

pour tout ouvert $\mathcal{U} \subset X$. Soient en effet $\{\mathcal{U}_\alpha\}$ un recouvrement ouvert de X et $(f_\alpha, g_\alpha) \in \mathcal{O}_1 \oplus \mathcal{O}(\mathcal{U}_\alpha)$ des sections tels que

$$f_\alpha|\mathcal{U}_\alpha \cap \mathcal{U}_\beta = f_\beta|\mathcal{U}_\alpha \cap \mathcal{U}_\beta$$

En particulier,

$$f_\alpha|\mathcal{U}_\alpha \cap \mathcal{U}_\beta = f_\beta|\mathcal{U}_\alpha \cap \mathcal{U}_\beta$$

$$g_\alpha|\mathcal{U}_\alpha \cap \mathcal{U}_\beta = g_\beta|\mathcal{U}_\alpha \cap \mathcal{U}_\beta$$

Aprés, on applique l'axiome des faisceaux à $\{f_\alpha\}$, $\{g_\alpha\}$ et l'unicité de l'ecriture en somme directe.

Exemple 8 : Produit tensoriel On définit le produit tensoriel de $\mathcal{O}_1$ par $\mathcal{O}_2$ comme étant le faisceaux $\mathcal{O}'$ sur X définit par :

$$\mathcal{O}(\mathcal{U}) = \mathcal{O}_1(\mathcal{U}) \otimes \mathcal{O}_2(\mathcal{U})$$

pour tout ouvert $\mathcal{U}$ de X. Neanmoins on peut montrer que le presfaisceau $\mathcal{O}$ n'est en général pas un faisceau.

Exemple 9 : Quotient Supposons que pour tout ouvert $\mathcal{U}$ on ait un idéal $\mathcal{I}(\mathcal{U})$ de $\mathcal{O}_1(\mathcal{U})$ alors on définit le quotient de $\mathcal{O}_1$ par $\mathcal{I}$ comme le faisceau $\mathcal{F}'$ donné par :

$$\mathcal{F}(\mathcal{U}) = \mathcal{O}_1(\mathcal{U})/\mathcal{I}(\mathcal{U})$$

pour tout ouvert $\mho \subset X$. On dénote $\mathcal{F}'$ par $\mathcal{O}_1/\mathcal{I}$. Ainsi tout morphisme de faisceaux $F : \mathcal{O}_1 \longrightarrow \mathcal{O}_2$ se factorise en un morphisme $\tilde{F} : \mathcal{O}_1/Ker(F) \longrightarrow \mathcal{O}_2$ où l'on note

$$Ker(F)(\mho) = Ker(F(\mho))$$

pour tout ouvert $\mho \subset X$.

En s'aidant des exemples précédents on peut vérifier que :

Proposition 8 *La catégorie des faisceaux sur X est abelienne.*

Soit $\mathcal{B}$ une base d'ouverts sur X. (i.e tout ouvert de X est réunion d'éléments de $\mathcal{B}$) Supposons que tous éléments $U \subset V$ de $\mathcal{B}$ on ait des anneaux $\mathcal{O}(U)$ et des applications restrictions $\rho_{V,U} : \mathcal{O}(V) \longrightarrow \mathcal{O}(U)$ vérifiant l'axiome suivant. Pour tout recouvrement d'ouverts $\{U_\alpha\}$ de X par des éléments de $\mathcal{B}$, si pour tout α, β il existe $s_\alpha \in \mathcal{O}(U_\alpha)$ et $s_\beta \in \mathcal{O}(U_\beta)$ tels que leurs restrictions à un élément de $\mathcal{B}$ inclus dans $U_\alpha \cap U_\beta$ soit égal alors il existe un unique $s \in \mathcal{O}(Z)$ tel que sa restriction à U_α soit s_α. Par suite, sous l'axiome précédent l'assignation

$$\mathcal{B} \ni \mho \longmapsto \mathcal{O}(\mho)$$

est appelée faisceau sur la base $\mathcal{B}$.

Exemple 10: Limite inductive Soit $\mathcal{O}$ un faisceau sur la base $\mathcal{B}$. Puisque l'ensemble des applications restrictions est un système inductif (voir la régle de cocycle), on peut donc définir la limite inductive $\lim_W \mathcal{O}(W)$ du système $\{\rho_{V,W}\}$ où les indices $V \subset W$ parcourent les éléments de $\mathcal{B}$ inclus dans $\mho$. Ainsi on pose :

$$\lim_W \mathcal{O}(W) = \mathcal{O}(\mho)$$

c'est donc l'anneau des familles $\{f_W, W \subset \mho\}$ telles que pour toute suite d'inclusions $W \subset V \subset \mho$ avec $W, V \in \mathcal{B}$ on ait :

$$\rho_{V,W} f_V = f_W$$

Cette dernière observation nous donne le resultat suivant :

Lemme 2 *Tout faisceau sur une base s'étend en un unique faisceau.*

Démonstration On note $\mathcal{O}$ la régle obtenue par limite inductive comme ci-dessus. Soient $U \subset V$ deux ouverts quelconques, on définit le morphisme $\rho_{V,U} : \mathcal{O}(V) \longrightarrow \mathcal{O}(U)$ par :

$$\rho_{V,U}\{f_T, T \subset V\} = \{\rho_{V,U} f_T, T \subset V\}$$

Donc, si W est un troisième ouvert contenant V alors :

$$\rho_{V,U} \circ \rho_{W,V}\{f_T, T \subset W\} = \{\rho_{V,U} \circ \rho_{W,V} f_T, T \subset U\} =$$

$$\{\rho_{W,U} f_T, T \subset U\} = \rho_{W,U}\{f_T, T \subset W\}$$

Ce qui montre que $\mathcal{O}$ est un presfaisceau. Ensuite, si $\{\mho_\alpha\}$ est un recouvrement ouvert de X et $\{f_\alpha \in \mathcal{O}(\mho_\alpha)\}$ une famille de sections telle que les restrictions de f_α et f_β à $\mho_\alpha \cap \mho_\beta$ soient égales alors en rafinant la famille $\{\mho_\alpha\}$ à des éléments de $\mathcal{B}$, on a le résultat par définition des faisceaux sur la base $\mathcal{B}$.

1.1.3 Partition de l'unité

Soit R un anneau quelconque. On note $Spec(R)$ l'ensemble des idéaux premiers de R et pour une partie S de R, $V(S)$ l'ensemble des idéaux premiers contenant S. Puisque

$$V(S) = \bigcap_{f \in S} V(\{f\})$$

les $V(S)$ forment une topologie dite spectrale. Cette topologie est parfois appelée topologie de Zariski pour la raison suivante. Soit f un élément de R, on sous-entend f comme une "fonction" de $Spec(R)$ dont la valeur en un idéal premier $\mathfrak{p}$ est l'image de f par les morphismes canoniques

$$R \longrightarrow R/\mathfrak{p} \longrightarrow k(\mathfrak{p})$$

où $k(\mathfrak{p})$ est le corps de fraction de l'anneau $R/\mathfrak{p}$. Ainsi "l'ensemble algébrique"

$$\{\mathfrak{p} \in Spec(R) | \forall f \in S, f(\mathfrak{p}) = 0\}$$

est $V(S)$.

Définition Soit S une partie multiplicative de R. On appelle localisé de R par rapport à S l'ensemble $S^{-1}R$ des fractions a/s où on identifie deux représentants $(a, s), (b, r) \in R \times S$ de a/s s'il existe $u \in S$ tel que $u(ar - bs) = 0$.

$S^{-1}R$ munit des régles d'addition et de multiplication habituelles sur les fractions est un anneau. On rappelle qu'un anneau local est un anneau qui posséde un unique idéal maximal et que le quotient par celui-ci est appelé corps résiduel.

Proposition 9 *Si S est le complémentaire d'un idéal $\mathfrak{p}$ alors $S^{-1}R$ est un anneau local d'idéal maximal $\mathfrak{p}S^{-1}R$ dont le corps residuel est le corps de fractions k de $R/\mathfrak{p}$.*

Démonstration On observe que le complémentaire de $\mathfrak{p}S^{-1}R$ est inclus dans les inversibles $S^{-1}R^\times$, car si $a/s \notin \mathfrak{p}S^{-1}R$ alors $a \in S$ et $s/a \in S^{-1}R$. Donc $S^{-1}R$ est local. Ensuite, soit ϕ le morphisme qui à chaque $a/s \in S^{-1}R$ associe $a/s \in k$. Alors ϕ est surjectif de noyau $\mathfrak{p}S^{-1}R$.

Pour alléger les notations, on dénote par $V(f)$ le fermé $V(\{f\})$, $D(f)$ le complémentaire de $V(f)$ et R_f le localisé de R par rapport à la partie multiplicative des puissances de f. Notons que R_f est un anneau local.

Lemme 3 *$D(f)$ forme une base d'ouverts de $Spec(R)$. Il existe une bijection naturelle entre $Spec(R_f)$ et $D(f)$.*

Démonstration Soit $\mho$ un ouvert de $Z = Spec(R)$. Donc il existe une partie $S \subset Z$ telle que le complémentaire de $\mho$ soit $V(S)$. Donc

$$\mho = Z - V(S) = Z - \bigcap_{f \in S} V(f) = \bigcup_{f \in S} Z - V(f) = \bigcup_{f \in S} D(f)$$

D'où la première assertion. Soit $f \in R$. Ensuite on considére l'application

$$D(f) \ni \mathfrak{a} \longmapsto \mathfrak{a}R_f \in Spec(R_f)$$

qui est bien définie et est une bijection.

L'observation suivante est importante :

Lemme 4 *$Spec(R)$ pour la topologie spectrale est un espace topologique quasi-compact.*

Démonstration On remarque par le lemme précédent que tout recouvrement d'ouverts se ramifie en un recouvrement des ouverts distingués $D(f)$. Soit S un sous-ensemble de R tel que

$$Z = Spec(R) = \bigcup_{f \in S} D(f)$$

Donc en passant au complémentaire l'expression ci-dessus $V(S) = \emptyset$. Donc S engendre l'idéal unité. Donc il existe des éléments $a_1, ..., a_N$ de R et des éléments $f_1, f_2, ..., f_N$ de S tels que

$$1 = a_1 f_1 + a_2 f_2 + ... + a_N f_N$$

Donc $V(\{f_1, ..., f_N\}) = \emptyset$, ce qui s'ecrit encore :

$$Z = \bigcup_{i=1}^{N} D(f_i)$$

D'où le resultat.

Lemme 5 *Soient f, g deux éléments de R. Si $D(f)$ est inclus dans $D(g)$ alors on a un morphisme d'anneaux $\rho_{D(g),D(f)} : R_f \longrightarrow R_g$ naturel que l'on appelle restriction.*

Démonstration Par hypothése, en passant au complémentaire on a : $V(g) \subset V(f)$. Donc

$$\sqrt{(f)} = \bigcap_{\mathfrak{p} \in V(\{f\})} \mathfrak{p} \subset \bigcap_{\mathfrak{p} \in V(\{g\})} \mathfrak{p} = \sqrt{(g)}$$

Donc il existe un entier $N \geq 0$ et $a \in R$ tel que $f^N = ag$ et on pose :

$$\rho_{D(g),D(f)}(\frac{b}{g^k}) = \frac{a^k b}{(ag)^k}$$

Ce qui définit bien un morphisme d'anneaux de R_g vers R_f.

On note D la base d'ouverts de $Spec(R)$ formé par les ouverts $D(f)$. Pour tout $f \in R$ on note $\mathcal{O}(D(f)) = R_f$ et par la proposition précédente on a une application restriction :

$$\rho_{D(g),D(f)} : \mathcal{O}(D(g)) \longrightarrow \mathcal{O}(D(f))$$

lorsque $D(f)$ est inclus dans $D(g)$, il s'ensuit :

Théorème 2 *$\mathcal{O}$ est un faisceau d'anneaux sur la base D de $Spec(R)$ et s'etend donc en un unique faisceau que l'on appelle faisceau structural.*

Démonstration Nous faisons la démonstration en deux étapes :

(1) Soit $\{f_a\}$ une famille de R telle que les $D(f_a)$ recouvrent $Z = Spec(R)$. On peut supposer que cette famille est finie et qu'elle engendre R. Soient f, g deux éléments de R égaux dans R_{f_a} pour tout a, montrons que $f = g$ dans R. Donc pour tout a, il existe un entier positif $N(a)$ tel que

$$f_a^{N(a)}(g - f) = 0$$

Comme :

$$D(s^N) = Z - V(s^N) = Z - V(\sqrt{(s^N)}) = Z - V(\sqrt{(s)}) = Z - V(s) = D(s)$$

pour tout entier N posifif et tout $s \in R$, il s'ensuit que les $f_a^{N(a)}$ engendrent l'idéal unité. Donc il existe une famille finie $\{e_a\}$ de R telle que

$$\sum_a e_a f_a^{N(a)} = 1$$

Ce qui donne :

$$f - g = (\sum_a e_a f_a^{N(a)})(g - f) = 0$$

(2) Montrons que si pour tous a, b, on ait des fonctions g_a, g_b respectivement sur $D(f_a)$ et $D(f_b)$ telles que leurs restrictions à $D(f_a) \cap D(f_b) = D(f_a f_b)$ soient égales alors il existe g telle que sa restriction à $D(f_a)$ soit égale à g_a pour tout a. Tout d'abord, pour tout a, il existe un entier $N(a)$ positif tel que $f_a^{N(a)} g_a$ soit un élément h_a de R. Puisque que le nombre d'indice a est fini, quitte à changer h_a par un autre élément de R, on peut supposer que $N(a)$ est $N = max_a N(a)$. Ainsi par hypothèse :

$$f_b^N h_a = (f_b f_a)^N g_a = (f_a f_b)^N g_b = f_a^N h_b$$

pour tous a et b. En outre, par (1), il existe $d_a \in R$ pour tout a tel que

$$\sum_a d_a f_a^N = 1$$

Donc on pose :

$$g = \sum_a d_a h_a$$

Par suite, en utilisant un calcul précédent :

$$f_b^N g = \sum_a d_a f_b^N h_a = (\sum_a d_a f_a^N) h_b = h_b$$

Donc la restriction de g à $D(f_a)$ est égale à g_a

Epilogue Enfin, en utilisant (1), on observe que g est déterminé de manière unique et donc que $\mathcal{O}$ est un faisceau sur la base D.

Définition On appelle schéma affine le spectre d'un anneau muni de son faisceau structural.

1.1.4 Schéma

Soit X un espace topologique et $\mathcal{O}$ un faisceau d'anneaux sur X. Pour définir la notion de schéma et de morphisme de schémas, nous avons besoin des définitions :

Définition On dit que $(X, \mathcal{O})$ est un espace localement annelé si pour tout point $x \in X$ l'anneau $\mathcal{O}_x$ des germes en x est un anneau local d'idéal maximal $\mathfrak{m}_x$.

Soient x un point de X et f une section globale de $\mathcal{O}(X)$. On appelle valeur de f au point x que l'on dénote par $f(x)$ l'image de f par les morphismes canoniques

$$\mathcal{O}(X) \longrightarrow \mathcal{O}_x \longrightarrow k(x) = \mathcal{O}_x/\mathfrak{m}_x$$

En particulier, on dit que f s'annule en x lorsque $f(x) = 0$.

Exemple 1: Fonctions holomorphes On munit $\mathbb{C}$ du faisceau $\mathcal{O}$ d'anneaux des fonctions holomorphes. Si w est un nombre complexe alors $\mathcal{O}_w$ est un anneau local d'idéal maximal $\mathfrak{m}$ formé des fonctions f de $\mathcal{O}_w$ telles que $f(w) = 0$. En effet, si $f(w) \neq 0$ alors on peut trouver un petit disque $D \subset \mathbb{C}$ contenant w tel que pour tout $z \in D$, $f(z) \neq 0$ et la classe $[D, f|D]$ a pour inverse $[D, f^{-1}|D]$. Ainsi, le morphisme qui à toute germe $[\mathfrak{V}, f]$ associe $f(w)$ induit un isomorphisme entre $\mathcal{O}_w/\mathfrak{m}$ et les nombres complexes $\mathbb{C}$.

Soient R un anneau et $\mathfrak{p}$ un idéal premier de R. On dénote par $R_\mathfrak{p}$ le localisé de R par rapport àu complémentaire de $\mathfrak{p}$.

Proposition 10 *Un schéma affine est un espace localement annelé.*

Démonstration On remarque que $\mathcal{O}_p$ est la limite inductive des $\mathcal{O}(\mathfrak{V})$ où $\mathfrak{V}$ parcourt les ouverts contenant $\mathfrak{p}$. Pour cela on se restreint aux ouverts $D(f)$ avec $f \notin \mathfrak{p}$.

La proposition suivante montre l'analogie entre variétés algébriques et schémas affines.

Proposition 11 *Soient $X = Spec(R)$ un schéma affine et $\mathfrak{V}$ un ouvert de X. Alors $f \in \mathcal{O}(\mathfrak{V})$ si et seulement si pour tout point $\mathfrak{p}$ de $\mathfrak{V}$, il existe un ouvert $W \subset \mathfrak{V}$ contenant $\mathfrak{p}$ et $a, s \in R$ avec $s(\mathfrak{q}) \neq 0$ pour tout $\mathfrak{q}$, tel que : $f = a/s$.*

Démonstration En fait, si $\mathcal{O}$ est le faisceau structural de $Spec(R)$ alors $\mathcal{O}' = \mathcal{O}$ et donc le résultat est une conséquence de la déscription des sections de $\mathcal{O}'(\mathfrak{V})$ pour tout ouvert $\mathfrak{V}$.

Définition Soient $(X, \mathcal{O})$ un espace localement annelé. Pour toute fonction $f \in \mathcal{O}(X)$, on note $\mathfrak{V}_f$ l'ensemble des points y tel que l'image de f par le morphisme naturel

$$\mathcal{O}(X) \longrightarrow \mathcal{O}_y$$

soit un élément inversible de $\mathcal{O}_y$. L'espace $(X, \mathcal{O})$ est dit affine si :

(AFF1) pour toute section globale f, $\mathfrak{V}_f$ est un ouvert et $\mathcal{O}(\mathfrak{V}_f)$ est isomorphe à $\mathcal{O}(X)_f$.

(AFF2) pour tout point x de X le morphisme d'anneaux

$$\phi : \mathcal{O}(X) \longrightarrow \mathcal{O}_x$$

induit un homéomorphisme entre $Spec(\mathcal{O}(X))$ muni de sa topologie spectrale et l'espace topologique X définit par

$$X \ni x \longmapsto \phi^{-1}(\mathfrak{m}_x) \in Spec(\mathcal{O}(X))$$

où $\mathfrak{m}_x$ est l'idéal maximal de l'anneau local $\mathcal{O}_x$.

Un schéma affine est donc un espace localement annelé affine. De ce fait puisque la restriction à un ouvert d'un espace localement annelé est un espace localement annelé, on peut définir la notion de schéma en général comme un espace recouvert par des "ouverts affines".

Définition On appelle schéma un espace localement annelé $(X, \mathcal{O})$ tel que pour tout point x de X, il existe un ouvert $\mho$ contenant x tel que l'espace localement annelé $(\mho, \mathcal{O}|\mho)$ soit affine.

Donnnons quelques exemples :

Exemple 2: $Spec(\mathbb{Z})$ **-** Chaque idéal premier de $\mathbb{Z}$ est engendré par un entier premier ou nul. Si p est un nombre premier alors :

$$\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} | b \wedge p = 1\}$$

et

$$\mathbb{Z}_{(0)} = \mathbb{Q}$$

D'où, on tire : $k((0)) = \mathbb{Q}$ et $k((p)) = \mathbb{Z}/p\mathbb{Z}$. Ce qui montre que chaque point de $Spec(\mathbb{Z})$ a des germes de natures differentes.

Exemple 3 : $Spec(\mathbb{C}[T])$ **-** On considére l'anneau des polynômes $\mathbb{C}[T]$ à une indéterminée. Les idéaux premiers de $\mathbb{C}[T]$ sont representés par 0 et les polynômes de la forme $T - a$ avec $a \in \mathbb{C}$. Par conséquent :

$$\mathbb{C}[T]_{(T-a)} = \{P/Q \in \mathbb{C}(T) | Q(a) \neq 0\}$$

qui représente les fractions rationnelles sans poles en a et

$$\mathbb{C}[T]_{(0)} = \mathbb{C}(T)$$

Neanmoins à la difference de $Spec(\mathbb{Z})$ chaque corps residuel est isomorphe aux fractions rationnelles $\mathbb{C}[T]$.

Définition Soient X, Y deux schémas on appelle morphisme de schémas un couple $(\psi, \psi^\sharp)$ formé d'une application $\psi : X \longrightarrow Y$ continue et d'un morphisme de faisceaux $\psi^\sharp : \mathcal{O}_Y \longrightarrow \psi_* \mathcal{O}_X$ tels que pour tout point $x \in X$ et tout ouvert $\mho \subset Y$ contenant $\psi(x)$, une section de s de $\mathcal{O}_Y(\mho)$ s'annule si et seulement si la section $\psi^\sharp(\mho)(s)$ de $\psi_* \mathcal{O}_X(\mho) = \mathcal{O}_X(\psi^{-1}(\mho))$ s'annule.

Soient $x \in X$ et $y = \psi^\sharp(x)$. La condition précédente traduit que $\psi^\sharp$ induit un morphisme d'anneaux :

$$\psi_y^\sharp : \mathcal{O}_y \longrightarrow \mathcal{O}_x$$

tel que $\psi_y^\sharp(\mathfrak{m}_y) = \mathfrak{m}_x$. Nous laissons le soin au lecteur de vérifier que l'application identité et la composée de deux morphismes de schémas est un morphisme schémas.

Exemple 4 : Morphisme d'anneaux Si $g : R \longrightarrow S$ est un morphisme d'anneaux alors g induit un morphisme de schémas de $Spec(S)$ vers $Spec(R)$. En effet, on remarque (avec les mêmes notations que ci-dessus) que :

$$\psi = Spec(g) : \mathfrak{p} \in Spec(S) \longmapsto g^{-1}(\mathfrak{p}) \in Spec(R)$$

et que :

$$\psi^\sharp(D(f)) = g_f : R_f \ni a/f^N \longmapsto g(a)/g(f)^N \in S_{g(f)}$$

En particulier, $\psi^\sharp(Spec(R)) = g$. On conclut en utilisant la limite inductive. Ainsi la régle F de la catégorie des anneaux vers la catégorie des schémas telle que $F(R) = Spec(R)$ et qui à tout tout morphisme $g : R \longrightarrow S$ associe

$$(Spec(g), (\lim_{D(f)\subset\mho} g_f)_\mho) : Spec(S) \longrightarrow Spec(R)$$

est un foncteur contravariant. Notons F^o le foncteur construit à partir de F de la catégorie opposée des anneaux vers celle des schémas affines. F^o admet un inverse donné par $G(Spec(R)) = R$ et pour tout morphisme $(\psi, \psi^\sharp) : Spec(S) \longrightarrow Spec(R)$ associe

$$[\psi^\sharp(Spec(R))]^o : S \longrightarrow R$$

On obtient ainsi un résultat qui sera important par la suite :

Théorème 3 *La catégorie des schémas affines est equivalente à la catégorie opposée des anneaux.*

Notons que deux spectres d'anneaux peuvent être isomorphe en tant qu'espaces topologiques mais pas en tant que schémas affines. En effet, $Spec(\mathbb{Q})$ et $Spec(\mathbb{F}_2)$ sont deux espaces topolgiques identiques mais il n'existe pas de morphisme d'anneaux entre $\mathbb{Q}$ et $\mathbb{F}_2$.

Exemple 5 : Droite réelles et complexes Soient T une variable et $f : \mathbb{R}[T] \longrightarrow \mathbb{C}[T]$ l'inclusion. Alors f induit un morphisme de schémas de

$$Spec(\mathbb{C}[T]) \longrightarrow Spec(\mathbb{R}[T])$$

défini de la manière suivante :

$$\psi : Spec(\mathbb{C}[T]) \ni (T-a) \longrightarrow f^{-1}(T-a) \in Spec(\mathbb{R}[T])$$

Si a est réel alors :

$$\psi((T-a)\mathbb{C}[T]) = (T-a)\mathbb{R}[T]$$

Sinon $a = \alpha \mp i\beta$ n'est pas réel (avec $\alpha, \beta \in \mathbb{R}$) et :

$$\psi((T-a)\mathbb{C}[T]) = (T^2 - 2\alpha T + \alpha^2 + \beta^2)\mathbb{R}[T]$$

Donc la droite réelle $Spec(\mathbb{R}[T])$ moins le point générique (0) s'identifie au plan superieur des nombres complexes de parties réelles positives. En outre si $P \in \mathbb{R}[T]$ alors :

$$\psi^\sharp(D(P)) : \mathbb{R}[T]_P \longrightarrow \mathbb{C}[T]_P$$

Exemple 5 : Schéma sur $Spec(K)$ Soit K un corps. On note $\mathfrak{K}$ la catégorie dont les objets sont des morphismes $f : Spec(R) \longrightarrow Spec(K)$ de schémas affines et les morphismes entre deux objets f et $g : Spec(S) \longrightarrow Spec(K)$ sont les morphismes de schémas $h : Spec(R) \longrightarrow Spec(S)$ tels que $h \circ g = f$. Soit $Z = Spec(A)$ un schéma affine. Par ailleurs, on vérifie que $u : Z \longrightarrow Spec(K)$ est un morphisme si et seulement si u est un morphisme de K vers $k_Z(\mathfrak{p})$ pour tout $\mathfrak{p} \in Spec(A)$.

Exemple 6 : Parabole Soient K un corps et X, Y, T des indéterminées. Alors la parabole $Spec(K[X,Y]/(Y - X^2))$ est isomorphe à la droite affine $Spec(K[T])$. En effet, on considére le morphisme d'anneaux :

$$f : K[X,Y] \ni P(X,Y) \longmapsto P(T,T^2) \in K[T]$$

est surjectif, de noyau $(Y - X^2)$ et induit donc un isomorphisme de $K[X,Y]/(Y - X^2)$ vers $K[T]$. Ensuite, on conclut par le théorème précédent.

Corollaire 1 *La catégorie opposée des algébres sur* K *est equivalente à la catégorie* $\mathfrak{S}(K)$ *des schémas affine sur* $Spec(K)$.

Exemple 7 : Groupe de Galois Soit K/L un extension galoisienne de groupe de Galois $G_{K/L}$ alors l'ensemble des automorphismes de $Spec(K) \longrightarrow Spec(L)$ dans la catégorie $\mathfrak{S}(L)$ est un groupe isomorphe à $G_{K/L}$. En particulier, si L est un corps premier, $G_{K/L}$ s'identifie aux automorphismes de $Spec(K)$. Donc bien que $Spec(K)$ ait un seul élément, il possède en gén éral plus d'un automorphisme.

Exemple 9 : $Spec(\mathbb{Q}[T])$ **-** Soit T une variable et $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$. Alors pour compléter l'exemple 5 le lecteur pourra vérifier que $Spec(\mathbb{Q}[T])$ moins le point générique est en bijection avec les orbites de l'action du groupe de Galois absolue $G_{\overline{\mathbb{Q}}/\mathbb{Q}}$ sur les nombres algébriques $\overline{\mathbb{Q}}$.

Exemple 10 : Ouvert Soit $\mho$ un ouvert d'un schéma X alors l'espace localement annelé $(\mho, \mathcal{O}_X|\mho)$ est un schéma. En effet, on peut recouvrir X et donc $\mho$ par des ouverts affines $W_\alpha = Spec(R_\alpha)$. Ensuite, on écrit :

$$W_\alpha = \bigcup_{f \in R_\alpha} D_\alpha(f)$$

$$Z = \bigcup_{\alpha} R_\alpha$$

Aprés, on note S l'ensemble des couples (α, f) où $f \in Z$ tel que $D_\alpha(f) \subset \mho$. Donc pour tout $(\alpha, f) \in S$:

$$\mathcal{O}_X|\mho(D_\alpha(f)) = \mathcal{O}_X(D_\alpha(f)) = R_{\alpha,f}$$

Ce qui montre que $\mho$ est recouvert par des espaces affines.

Exemple 11 : Fermé Si $Spec(R)$ est un schéma affine et $\mathfrak{a}$ un idéal de R alors on a une inclusion

$$V(\mathfrak{a}) = Spec(R/\mathfrak{a}) \longrightarrow Spec(R)$$

qui provient du fait que les idéaux de $R/\mathfrak{a}$ sont en bijection avec les idéaux contenant $\mathfrak{a}$. Donc $Spec(R/\mathfrak{a})$ est donc un sous-schéma fermé de $Spec(R)$. De manière général on peut définir la notion de sous-schéma fermé à l'aide de quotient de faiceau d'anneaux.

Nous donnons maintenant des exemples de schémas non affine

Exemple 12 : Recollement

Exemple 13 : Schémas projectifs

1.2 Schéma en groupe affine

1.2.1 Produit fibré et somme almalgamée

Nous introduisons une notion qui permet de généraliser les notions ensemblistes de produit catésien, intersection, union et préimage au sein de diverses catégories.

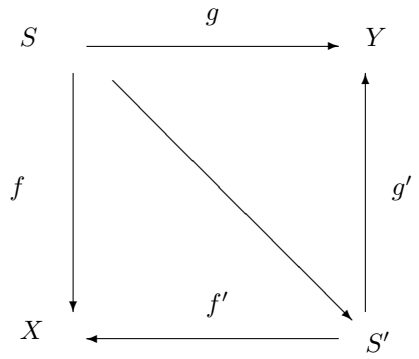
Soient $\mathfrak{A}$ une catégorie et X, Y des objets de $\mathfrak{A}$.

Définition On note $\mathfrak{A}_{X,Y}$ la catégorie dont les objets sont des paires de morphismes

$$f : S \longrightarrow X$$

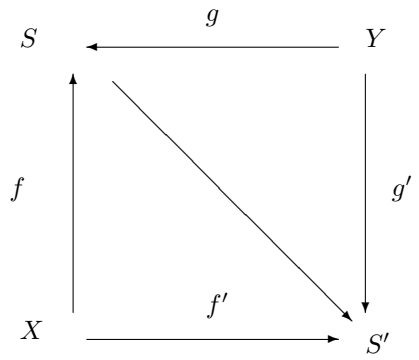
$$g : S \longrightarrow Y$$

pour tous objets X, Y, S et dont un morphisme (f, g) vers $(f', g') : S' \longrightarrow X, Y$ est un morphisme $h : S \longrightarrow S'$ tel le diagramme suivant



soit commutatif

Définition De manière similaire, on note $\mathfrak{A}^{X,Y}$ la catégorie formée des couples de morphismes $(f, g) : X, Y \longrightarrow S$ tels qu'un morphisme de (f, g) vers $(f', g') : X, Y \longrightarrow S'$ soit un morphisme $h : S \longrightarrow S'$ tel que le diagramme suivant



soit commutatif.

Les produits et de sommes apparaîssent comme objets universels au sein des catégories $\mathfrak{A}_{X,Y}$ et $\mathfrak{A}^{X,Y}$:

Définition Un produit X par Y dans $\mathfrak{A}$ est la donnée d'un objet $(f,g) : P \longrightarrow X,Y$ de $\mathfrak{A}_{X,Y}$ tel que pour tout objet $(u,v) : S \longrightarrow X,Y$, il existe un unique morphisme de (u,v) vers (f,g).

L'unicité des objets universaux à isomorphisme près montre que notre définition a un sens :

Proposition 12 *S'il existe un produit (f,g) dans $\mathfrak{A}$ formé par deux objets X,Y de $\mathfrak{A}$ alors un autre produit de X par Y est isomorphe à (f,g) dans la catégorie $\mathfrak{A}_{X,Y}$.*

Donnons un exemple :

Proposition 13 *Le produit direct est un produit dans la catégorie des groupes.*

Démonstration Soient G,S,T des groupes, $S \times T$ le produit direct de S et T, $(u,v) : G \longrightarrow S,T$ une paire de morphisme et $(p_1,p_2) : S \times T \longrightarrow S,T$ les projections naturelles. Donc le morphisme de groupes

$$w : G \ni x \longmapsto (u(x),v(x)) \in S \times T$$

est un morphisme de (u,v) vers (p_1,p_2). Si f est un autre morphisme de (u,v) vers (p_1,p_2) alors il doit satisfaire $p_1 \circ f = u$ et $p_2 \circ f = v$ ce qui force $f = w$.

Définition Une somme de X par Y dans $\mathfrak{A}$ est la donnée d'un objet (f,g) de $\mathfrak{A}^{X,Y}$ tel que pour tout objet (u,v), il existe un unique morphisme de (f,g) vers (u,v).

Pour l'unicité de la somme les mêmes arguments s'appliquent. Par ailleurs, des définitions ci-dessus on a :

Proposition 14 *P est un produit de X par Y dans $\mathfrak{A}$ si et seulement si P est une somme de X par Y dans la catégorie opposée $\mathfrak{A}^o$.*

Voici un exemple fondamental de somme :

Proposition 15 *Le produit tensoriel est une somme dans la catégorie des anneaux.*

Démonstration Soient A,S,T des anneaux et $(u,v) : A \longrightarrow S,T$ un couple de morphismes d'anneaux. On considére les morphismes naturels :

$$s_1 : S \ni x \longmapsto x \otimes 1 \in S \otimes T$$

$$s_2 : T \ni y \longmapsto 1 \otimes y \in S \otimes T$$

et le morphisme w de (u,v) vers (s_1,s_2) définit par :

$$w : S \otimes T \ni \sum_{\alpha,\beta} x_\alpha \otimes y_\beta \longmapsto \sum_{\alpha,\beta} u(x_\alpha)v(y_\beta) \in A$$

Soient $x,y \in A$. Si s est un autre morphisme de (u,v) vers (s_1,s_2) alors s satisfait $s(x \otimes 1) = u(x)$ et $s(1 \otimes y) = v(y)$. Donc :

$$s(x \otimes y) = s((x \otimes 1)(1 \otimes y)) = u(x)v(y)$$

Donc si $\sum x_\alpha \otimes y_\beta \in S \otimes T$ alors

$$s(\sum x_\alpha \otimes y_\beta) = \sum s(x_\alpha \otimes y_\beta) = \sum u(x_\alpha)v(y_\beta) = w(\sum x_\alpha \otimes y_\beta)$$

D'où $s = w$.

Définition Soit S un objet de $\mathfrak{A}$. On appelle catégorie des objets de $\mathfrak{A}$ au-dessus de S la catégorie notée $\mathfrak{A}_S$ dont les objets sont des morphismes $f : X \longrightarrow S$ et les morphismes de f vers $g : Y \longrightarrow S$ est un morphisme $h : X \longrightarrow Y$ tel que $g \circ h = f$. De manière analogue, on note $\mathfrak{A}^S$ la catégorie opposée de $\mathfrak{A}_S$ dite des objets de $\mathfrak{A}$ en-dessous de S.

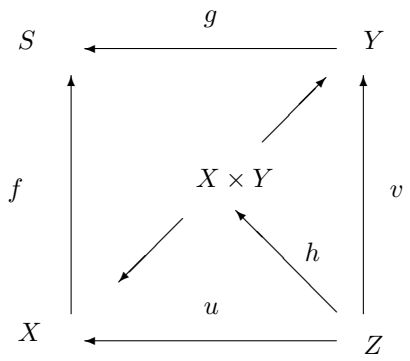
On vient à la notion centrale :

Définition Soit S un objet de $\mathfrak{A}$ et f, g deux éléments de $\mathfrak{A}_S$. On appelle produit fibré de f par g dans $\mathfrak{A}$ un produit de f par g dans la catégorie $\mathfrak{A}_S$. De même, on appelle somme amalgamée une somme dans la catégorie $\mathfrak{A}^S$.

Dans la catégorie des ensembles $\mathfrak{Ens}$ ceci se traduit par :

Proposition 16 *Soit $(f, g) : X, Y \longrightarrow S$ un objet de $\mathfrak{Ens}^{X,Y}$. Si l'on note $X \times_S Y$ l'ensemble des couples (x, y) de $X \times Y$ tel que $f(x) = g(y)$ et $p_X, p_Y : X \times_S Y \longrightarrow X, Y$ les projections naturelles alors (p_1, p_2) est un produit fibré.*

Démonstration On considère le diagramme commutatif :



qui est bien défini par définition de $X \times_S Y$. Notons $(u, v) : Z \longrightarrow X, Y$ les flèches ci-dessus, il s'agit de montrer que h est déterminé de manière unique. Puisque l'image de u et v est contenu dans celle des projections naturelle $X \times_S Y \longrightarrow X, Y$. Pour tout $x \in Z$, on a :

$$f \circ u(x) = g \circ v(x)$$

ce qui montre que l'application :

$$Z \ni x \longmapsto (u(x), v(x)) \in X \times_S Y$$

est bien définie et est par commutativité du diagramme h.

En fait, le produit fibré véhicule beaucoup d'informations :

Proposition 17 *Soient X, Y, S des ensembles et $X \times_S Y$ le produit fibré donné par les applications $(f, g) : X, Y \longrightarrow S$. Si S est un singleton alors $X \times_S Y = X \times Y$. Si $X, Y \subset S$ et f, g sont les inclusions alors $X \times_S Y = X \cap Y$. Si $Y \subset S$ et g est l'inclusion alors $X \times_S Y = f^{-1}(Y)$.*

Si $\mathfrak{Ann}$ désigne la catégorie des anneaux et S un anneau alors $\mathfrak{Ann}^S$ correspond à la catégorie des algébres sur S.

Proposition 18 *Le produit tensoriel des algébres sur S est une somme amalgamée.*

Démonstration La démonstration est identique à celle faite pour les anneaux.

Puisque l'image d'une somme par un foncteur contravariant est un produit, la proposition précédente implique l'existence d'un produit dans la catégorie des schémas affines sur un autre :

Corollaire 2 *Si est R un anneau et $\mathfrak{S}(R)$ la catégorie des schémas affines au dessus de $Spec(R)$ alors le produit deux morphismes $Spec(S), Spec(T) \longrightarrow Spec(R)$ est donné par $Spec(S \otimes_R T) \longrightarrow Spec(S), Spec(T)$.*

Donnons un exemple concret. Soient X, Y deux variables et K un corps. Alors on a l'isormorphisme naturel $K[X] \otimes K[Y] \cong K[X, Y]$ qui à $X \otimes Y$ associe XY. Donc on obtient $Spec(K[X]) \times Spec(K[Y]) = Spec(K[X, Y])$. Ce qui sinifie que le produit de deux droites affines est le plan affine.

1.2.2 Foncteur de points

Nous partons de l'intuition suivante. Si R est une algébre (commutative unifère) sur un annneau B alors R est construite à l'aide d'une famille de polynômes. En effet, soient $\{x_\alpha\}$ des générateurs de R (On peut prendre $\{x_\alpha\} = R$) et $X = \{x_\alpha\}$ une famille d'indéterminées toutes indexées sur le même ensemble. Donc le morphisme

$$B[X] \longrightarrow R$$

envoyant X_α sur x_α est surjectif et de noyau N engendré par une famille de polynômes $\{P_\beta\}$. Donc $B[X]/N \cong R$. Soit maintenant A une autre algébre sur B alors les morphismes d'algébres $Hom_B(B[X]/N, A)$ correspondent bijectivement aux solutions $a = (a_\alpha)$ dans A telles que pour tout β, $P_\beta(a) = 0$. Car tout morphisme est uniquement déterminé par les valeurs des classes X_α modulo N. De plus, une solution donne un morphisme de la même façon. Par ailleurs, pour le cas où $B = K$ est un corps algébriquement clos, R de type fini et $A = K$, on a la bijection :

$$Hom_K(R, K) \longrightarrow Z(N)$$

Définition Un foncteur d'une catégorie $\mathfrak{A}$ vers les ensembles $\mathfrak{Ens}$ est dit représentable s'il est isomorphe à un foncteur dont l'assignation entre objets est :

$$A \longmapsto h_S(A) = Hom_{\mathfrak{A}}(S, A)$$

et dont celle entre flèches est :

$$f \longmapsto h_S(f) : g \mapsto f \circ g$$

Soit B un anneau. Nous rappelons que toute nos algébres sont associatives, commutatives et unifères

Définition On appelle foncteurs de points sur B un foncteur représentable de la catégorie des algébres sur B vers celle des ensembles.

L'approche des foncteurs de points est justifiée par le lemme suivant dit de Yoneda :

Lemme 6 *Si $F : \mathfrak{A} \longrightarrow \mathfrak{Ens}$ est un foncteur covariant alors on a une bijection entre les transformation $Hom(h_A, F)$ vers les points de $F(A)$ donnée par l'application :*

$$\psi \longmapsto \psi(A)(id_A)$$

En outre; on a : $Hom(A, B) \cong Hom(h_B, h_A)$ pour tout objet B de $\mathfrak{A}$.

Démonstration L'application donnée par l'enoncé admet pour inverse l'application

$$F(A)$$

Pour le deuxième point, il suffit de remplaçer F par h_B dans l'expression $Hom(h_A, F) \cong F(A)$.

Corollaire 3 *La catégorie des foncteurs de points sur B est équivalente à celle des schémas affines au dessus de B.*

Démonstration Par le lemme de Yoneda et par les axiomes de foncteurs on a : $R \cong S$ si et seulement si $h_R \cong h_S$ et $Hom(R, S) \cong Hom(h_S, h_R)$ pour toute algébres R et S sur B.

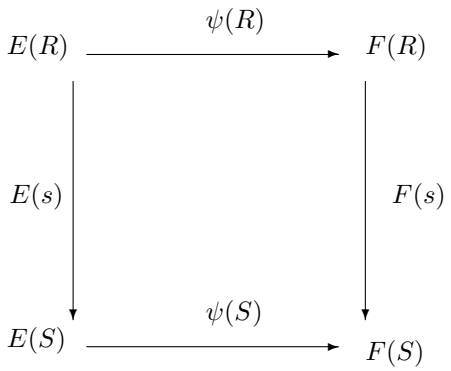
Nous pouvons à présent définir les schémas en groupe affine ainsi que leurs morphismes :

Définition Un schéma en groupe affine E de base B est un foncteur de points sur B à valeurs dans la catégorie des groupes. En d'autres termes pour toutes algébres R, S et morphisme $s : R \longrightarrow S$, $E(R)$ est un groupe et le morphisme naturel

$$h(f) : E(R) \longrightarrow E(S)$$

est un morphismes de groupes.

Définition Soient E, F deux schémas en groupe affines. Un mophisme de E vers F est une naturelle transformation $\psi : E \longrightarrow F$. Ce qui sinifie que pour toutes algébres R, S et morphisme $s : R \longrightarrow S$ sur B on a des morphismes de groupes $\psi(R) : E(R) \longrightarrow F(R)$ tels que le diagramme



soit commutatif.

Définition Soient $\psi_1 : E \longrightarrow G$ et $\psi_2 : F \longrightarrow G$ des morphismes entre schémas en groupe affines. On appelle produit fibrés de E par F selon les morphisme ci-dessus le foncteurs de groupes défini par :

$$E \times_C F(R) = \{(a, b) \in E(R) \times F(R) | \psi_1(a) = \psi_2(b)\}$$

Par suite, on a la conséquence directe provenant du paragraphe précédent :

Proposition 19 *Si E, F, G sont des schémas en groupe affines représentés par des algébres R, S et T alors le produit fibrés $E \times_C F$ selon les morphismes ψ_1, ψ_2 comme ci-dessus est un schéma en groupe affine représenté par le produit tensoriel $R \times_T S$ des algébres R, S sur T issues des morphismes ψ_1 et ψ_2.*

1.2.3 Algébre de Hopf

Bien que le résultat suivant se démontre par des arguments abstraits, nous le faisons explicitement afin d'effectuer des calculs uterieurement.

Proposition 20 *Si F est un schéma affine en groupe de base B représenté par une algébre S alors on a l'isomorphisme*

$$\phi_A : F(A) \times F(A) \longrightarrow Hom(S \otimes S, A)$$

qui tout couple de morphisme (f, g) associe le morphisme

$$S \otimes S \ni s \otimes s' \longmapsto f(s)g(s') \in A$$

pour tout algébre A sur B.

Démonstration Soit A une algébre sur B. Supposons que $\phi_A(f, g) = 0$ pour $f, g \in F(A)$ alors pour tous $s, s' \in S$

$$g(s) = \phi_A(g, h)(s \otimes 1) = 0 = \phi_A(g, h)(1 \otimes s') = h(s')$$

Donc ϕ_A est injectif. Soit $s \in S$. Si maintenant $f : S \times S \longrightarrow A$ est un morphisme alors on pose $g(s) = f(s \otimes 1)$ et $h(s) = f(1 \otimes s)$. Donc $\phi_A(g, h) = f$. Donc ϕ_A est un isomorphisme.

Définition On appelle algébre de Hopf la donnée d'une algébre A sur un anneau B et de morphismes $M : A \longrightarrow A \otimes A$, $I : A \longrightarrow A$ et $\varepsilon : A \longrightarrow B$ (dits respectivement comultiplication, coinverse et augmentation) satisfaisant les conditions suivantes. Soit $a \in A$. Si l'on note $M(a) = \sum a_\alpha \otimes b_\alpha$ avec $\otimes = \otimes_B$ alors :

(AH1)

$$\sum_\alpha M(a_\alpha) \otimes b_\alpha = \sum_\alpha a_\alpha \otimes M(b_\alpha)$$

(AH2)

$$\sum_\alpha S(a_\alpha) b_\beta = \varepsilon(a)$$

(AH3)

$$\sum_\alpha \varepsilon(a_\alpha) \otimes b_\alpha$$

$(AH1), (AH2)$ et $(AH3)$ sont appelés les axiomes de coassociativité, de coinverse et de coneutralité.

Le résultat suivant nous simplifie les calculs dans la partique :

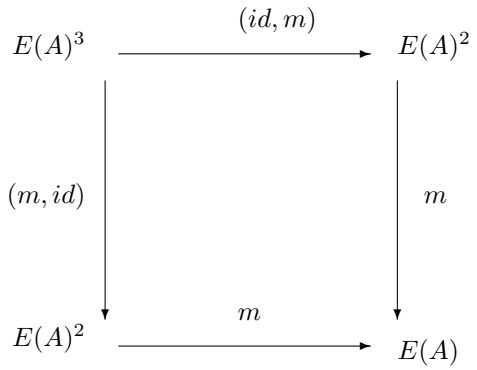
Proposition 21 *Soit A une algébre de type finie sur B. Alors A est une algébre de Hopf si et seulement si les relations $(AH1)$, $(AH2)$ et $(AH3)$ sont vérifées sur ses générateurs.*

Démonstration

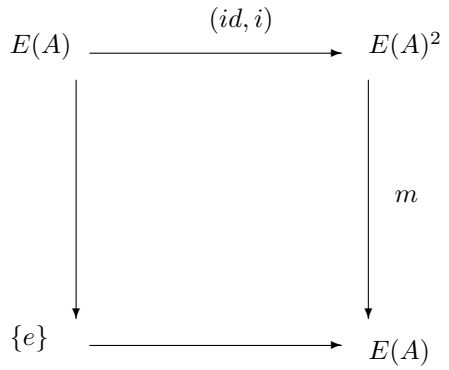
Définition Soient R, S deux algébres de Hopf sur le même anneaux. Un morphisme $s : R \longrightarrow S$ d'algébres est un morphisme d'algébres de Hopf si pour tout $x \in R$: $M \circ s(x) = s \circ M'(x)$, où M' et M sont respectivemement les comultiplications de R et S.

Proposition 22 *Les schémas affines en groupe de base B sont anti-équivalents aux algébres de Hopf sur B.*

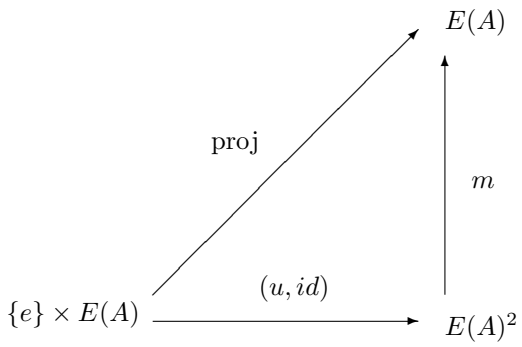
Démonstration Soit E un schéma affine en groupe de base B. Alors d'après le paragraphe précédent, E est un foncteur représentable de points muni des morphismes $m : E(A) \times E(A) \longrightarrow E(A), i : E(A) \longrightarrow E(A)$ et $u : \{e\} \longrightarrow E(A)$ avec A une algébre sur B et e un élément de $E(A)$ tels que l'on ait les diagrammes commutatifs :



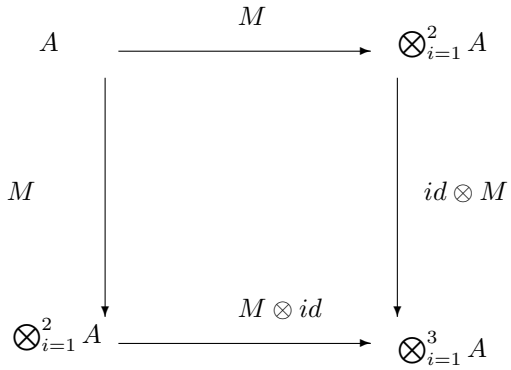
où pour tous $g, h, k \in E(A)$, $m(g, h)$ est noté gh, $(id, m)(g, h, k) = (g, hk)$, $(m, id)(g, h, k) = (gh, k)$,

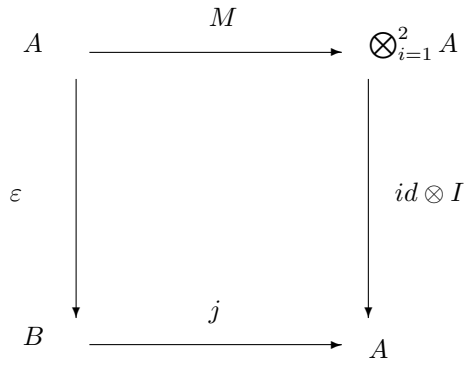


$(id, i)(g) = (g, g^{-1})$ pour tout $g \in E(A)$

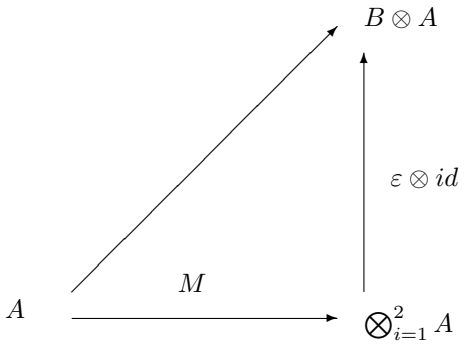


et $(u, id)(g) = (e, g)$ pour tout élément g de $E(A)$. Après puisque les algébres sont anti-équivalentes aux schémas en groupe affines, en retournant les diagrammes, on obtient :





($j : B \longrightarrow A$ étant le morphisme munissant A d'une structure d'algébre)



Ces derniers traduisent les axiomes d'algébres de Hopf. Enfin, on conclut en remarquant qu'un morphisme entre schéma en groupe est un morphisme qui préserve la multiplication ce qui correspond de manière bi-équivoque à un morphisme d'algébre préservant la comultiplication.

De la proposition précédente, on en déduit des propriétés analogue à celle des groupes que nous laissons en exercice :

Proposition 23 *Soit A une algébre de Hopf munie de ses morphismes M, I, ε. Alors : $I \circ I = id$, $\varepsilon \circ M = \varepsilon$ et l'application "cotranslation à droite" :*

$$A \otimes A \ni \sum_{\alpha} a_\alpha \otimes b_\alpha \longmapsto \sum_{\alpha} (a_\alpha \otimes 1) M(b_\alpha) \in A \times A$$

est un isomorphisme d'algébres de Hopf.

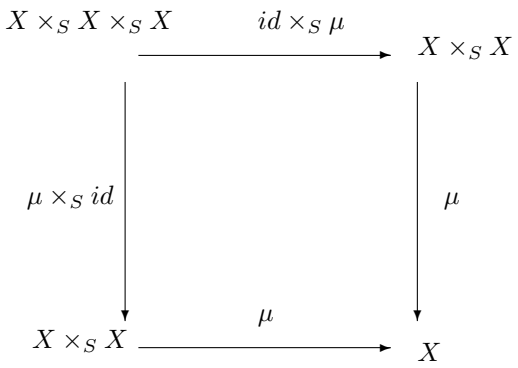
Définition Soient A une algébre de Hopf muni de la comultiplication M et $T : A \otimes A \longrightarrow A \times A$ le morphisme qui à tout tenseur élémentaire $a \otimes b$ associe $b \otimes a$. A est dite cocomutative si $T \circ M = M$.

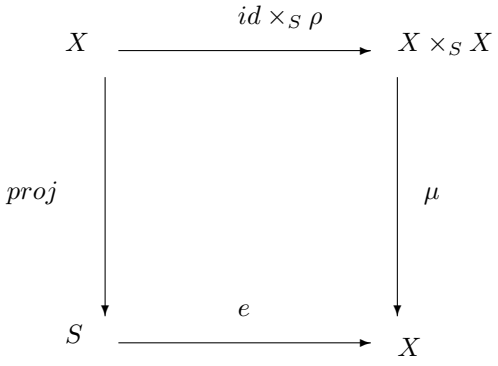
La vérification suivante est laissée aux lecteurs.

Proposition 24 *Soit E un schéma en groupe affine de base B représenté par une algébre de Hopf A. Alors $E(R)$ est commutative pour toute algébre R sur B si et seulement si A est cocomutative.*

Dans le cas de la proposition précédente, E est dit abélien. Notons $S = Spec(B)$. Afin de faire le lien ultérieurement avec les groupes algébriques nous proposons la définition suivante :

Définition alternative On appelle schéma en groupe affine de base B un schéma affine X au dessus de S muni de morphismes $e : S \longrightarrow X$, $\rho : X \longrightarrow X$ et $\mu : X \times_S X \longrightarrow X$ appelés respectivement identité, inverse et opération de groupe tels que les diagrammes :





(La projection $proj$ étant induite par le morphisme $j : B \longrightarrow A$ comme précédemment.)

En appliquant le foncteur $A \longmapsto Spec(A)$ aux algébres de Hopf sur B, il s'ensuit :

Proposition 25 *La catégorie des schémas en groupe affines de base B définie comme ci-dessus est anti-équivalente à celle des algèbres de Hopf.*

Donnons un exemple :

Exemple 1 : Le schéma en groupe G_a On considère le schéma en groupe affine G_a qui à toute algébre R associe le groupe additif R. G_a est représenté par $B[X]$ et on pour comultiplication : $M(X) = X \otimes 1 + 1 \otimes X$.

Exemple 2 : Le schéma en groupe G_m Le schéma en groupe affine G_m associe à toute algébre R le groupe des éléments inversibles $R^\times$. G_m est représenté par $B[X,Y]/(XY-1) = B[X,1/X]$ et a pour comultiplication : $M(X) = X \otimes X$.

Exemple 3 : Le schéma en groupe α_p On suppose que B est de caractérisique un nombre premier p. Pour toute algébre sur R, on note $\alpha_p(R)$ le groupe additif des éléments $x \in R$ tel que $x^p = 0$. α_p est un schéma en groupe affine représenté par $B[X]/(X^p)$ est de comultiplication : $M(X) = X \otimes 1 + 1 \otimes X$.

1.2.4 Le schéma en groupe GL_n

Le présent paragraphe est en lien avec la théorie des représentations. Nous proposons donc aux lecteurs de lire l'appendice sur les représentations complexes.

Soit B un anneau et n un entier ≥ 0. On considère le foncteur de groupes qui à toute algébre R sur B associe le groupe des matrices $GL_n(R)$ inversibles de type (n,n) à coefficients dans R. En effet, si S est une autre algébre et $\psi : R \longrightarrow S$ un morphisme d'algébres alors celui-ci induit une application $GL_m(\psi)$ qui à toute matrice $(a_{i,j})$ associe $(\psi(a_{i,j}))$. Soit $(a_{i,j}) \in GL_m(R)$. Alors ceci équivaut à

$$\det(a_{i,j}) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

inversible dans R et en appliquant ψ on déduit que $GL_n(\psi)$ est bien définie. En outre, puisque la multiplication de matrices est polynômiale en les coefficients de ses facteurs, il s'ensuit que $GL(\psi)$ est un morphisme de groupes.

En fait, on peut être plus précis :

Proposition 26 *GL_n est un schéma en groupe affine.*

Démonstration Par ce qui précéde, il suffit de montrer que GL_n est un foncteur de points. Pour i, j des entiers compris entre 1 et n, on note X_{ij} une indetérminé, X le système d'indéterminées fomé par tous les X_{ij} et Y une variable distincte des autres. Soit P le polynôme de $B[X, Y]$ défini par :

$$P(X, Y) = Y \det(X) - 1 = Y \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} X_{i,\sigma(i)} - 1$$

Notons $C = B[\det(X)^{-1}]$. On a l'isomorphisme naturel :

$$B[X, Y]/(P) \longrightarrow C[X]$$

Si maintenant R est une algébre sur B alors on a l'isomorphisme de groupes :

$$Hom_B(C[X], R) \ni \psi \longmapsto (\psi(X_{i,j})) \in GL_n(R)$$

Nous conservons la notation $X = (X_{i,j}; i, j = 1, ..., n)$ de la preuve ci-dessus.

Proposition 27 *Le schéma en groupe affine GL_n a pour algébre de Hopf $B[X, \det(X)^{-1}]$ de comultiplication M définie par :*

$$M(X_{i,j}) = \sum_{k=1}^{n} X_{i,k} \otimes X_{k,j}$$

pour tous entiers i, j compris entre 1 et n.

Démonstration Il reste à montrer que la comultiplication M définie comme ci-dessus est celle que l'on recherche. En effet, M est coassociative :

$$\sum_{k=1}^{n} M(X_{i,k}) \otimes X_{k,j} = \sum_{k=1} \sum_{l=1} X_{i,l} \otimes X_{l,k} \otimes X_{k,j} = \sum_{l=1} X_{i,l} M(X_{k,j})$$

Ensuite, soient $f, g : B[X, \det(X)^{-1}] \longrightarrow R$ deux morphismes vers une algébre R sur B. Posons $f(X_{i,j}) = (a_{i,j}) \in GL_n(R)$ et $g(X_{ij}) = (b_{i,j}) \in GL_n(R)$. Donc on a la suite de morphismes :

$$B[X, \det(X)^{-1}] \ni X_{i,j} \mapsto M(X_{i,j}) \in \bigotimes_{i=1}^{2} B[X, \det(X)^{-1}] \mapsto \sum_{k=1}^{n} a_{i,k} b_{k,j} \in R$$

Ce qui montre que la matrice $(X_{i,j})$ est envoyée sur le produit $(a_{i,j})(b_{i,j})$. Enfin, les morphismes coinverse et augmentation sont définis par :

$$\varepsilon(X_{i,j}) = (\delta_{i,j})$$

$$I(X_{ij}) = \frac{1}{\det(X_{i,j})} Cof(X_{i,j})^T$$

où $Cof(X_{i,j})$ est la matrice des cofacteurs de (X_{ij}). Ceci montre que $B[X, \det(X)^{-1}]$ est une algébre de Hopf, les morphismes ε et I étant unique.

Ainsi par cette même méthode, on retrouve le fait que l'inverse de $(X_{i,j})$ est un polynôme de $B[\det(X)^{-1}][X]$. Soit maintenant V un module sur l'anneau B. Pour tout algébre R sur B, on note $GL_V(R)$ le groupe $Aut_R(V \otimes R)$ des automorphismes linéaires sur R. On observe que si $u \in GL_V(R)$ alors u est entièrement déterminé par sa restriction à $V \otimes 1_R$. Par suite, si $x \in V$,

$$u(x \otimes 1_R) = \sum_\alpha x_\alpha \otimes a_\alpha$$

et $\psi : R \longrightarrow S$ est un morphisme d'algébres sur B alors on pose :

$$GL(\psi)(u)(x \otimes 1_S) = \sum_\alpha x_\alpha \otimes \psi(a_\alpha)$$

Après, si v est un autre élément de $GL_V(R)$ tel que :

$$v(x_\alpha \otimes 1) = \sum_\beta y_{\alpha,\beta} \otimes b_{\alpha,\beta}$$

pour tout α alors :

$$GL_V(\psi)(v \circ u)(x \otimes 1) = \sum_\alpha \sum_\beta y_{\alpha,\beta} \otimes \psi(a_\alpha b_{\alpha,\beta})$$

$$= \sum_\alpha \psi(a_\alpha) GL_V(\psi)(v)(x_\alpha \otimes 1) = GL_V(\psi)(v)(\sum_\alpha x_\alpha \otimes \psi(a_\alpha))$$

$$= GL_V(\psi)(v) \circ GL_V(\psi)(u)(x \otimes 1)$$

De plus,

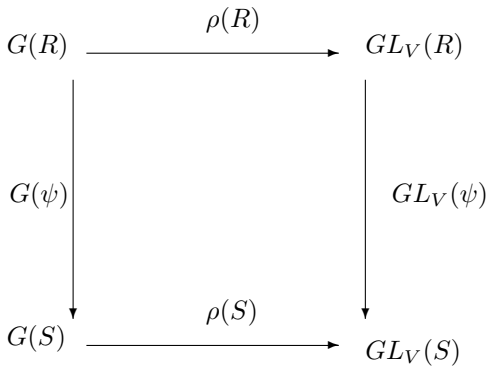
Proposition 28 *Si V est un module libre de type fini alors GL_V est un schéma en groupe affine.*

Démonstration En effet, si n est le rang de V alors $GL_V \cong GL_n$.

Désormais, V sera toujours un module libre de type fini.

Définition Une représentation d'un schéma en groupe affine G sur V est la donnée d'un morphisme $\rho : G \longrightarrow GL_V$.

Ce qui signifie que pour chaque algébre R, S, on a un morphisme $\rho(R) : G(R) \longrightarrow GL_V(R)$ tel que pour tout morphisme d'algébre $\psi : R \longrightarrow S$ on ait le diagramme commutatif :



Par ailleurs notons X le foncteur :

$$R \longmapsto X(R) = V \times R$$

Dés lors, une repésentation peut être définie comme une transformation naturelle $G \times X \longrightarrow X$ où telle que pour toute algébre R sur B

$$G(R) \times X(R) \longrightarrow X(R)$$

soit une action linéaire.

Exemple 1 : Une représentation de G_a Supposons que V soit de rang égal à 3. On considére la représentation ρ donnée :

$$g(av_1 + bv_2 + cv_3) = (a + cg)v_1 + (a + b + c)v_2 + av_3$$

avec v_1, v_2 et v_3 des vecteurs de base de V, $a, b, c \in R$ et $g \in G_a(R)$. La matrice associée est :

$$M(g) = \begin{pmatrix} 1 & 1 & g \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Cette dernière est inversible puisque son déterminant est égal à 1. En outre, ceci nous donne un morphisme entre algébres de Hopf :

$$B[X_{i,j}, \det(X)^{-1}] \longrightarrow B[T]$$

qui à tout $(X_{i,j})$ associe $M(g)$.

Soient A une algébre de Hopf sur B et M sa comultiplication.

Définition Soit W un module sur B. Une application linéaire $\rho : W \longrightarrow W \otimes A$ selon les scalaires B est un comodule si elle vérifie les conditions suivantes. Si l'on pose $\rho(v) = \sum_\alpha w_\alpha \otimes a_\alpha$ pour $v \in W$ alors :

(CO1)

$$\sum_\alpha w_\alpha \varepsilon(a_\alpha) = v$$

(CO2)

$$\sum_\alpha w_\alpha \otimes M(a_\alpha) = \sum_\alpha \rho(w_\alpha) \otimes a_\alpha$$

Par conséquent, on résume les axiomes $(CO1)$ et $(CO2)$ par $(id \otimes \varepsilon)\rho = id$ et $(id \otimes M)\rho = (\rho \otimes id)\rho$.

Exemple 2 : comultiplication L'application $M : A \longrightarrow A \otimes \otimes A$ est linéaire sur B et est un comodule.

Exemple 3 : Somme directe Soient $\rho_1 : W \longrightarrow W \otimes A$ et $\rho_2 : T \longrightarrow T \otimes A$ des comodules. Alors on pose :

$$\rho_1 \otimes \rho_2(u, v) = (\rho_1(u), \rho_2(v))$$

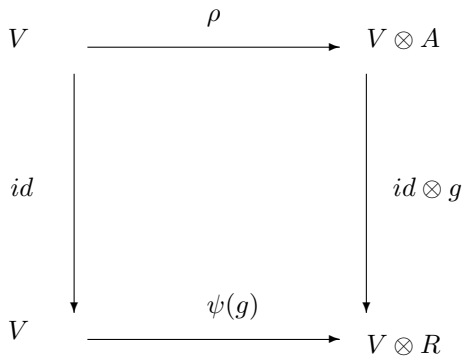
On vérifie de manière aisée que cela définit un comodule.

Définition Soient $\rho : W \longrightarrow W \otimes A$ un comodule et $T \subset W$ un sous-module. On dit que T est un sous-comodule si $\rho(T) \subset T \otimes A$.

On remarque alors que la restriction de ρ à T est encore un comodule. Le résultat suivant est important :

Théorème 4 *Si E est un schéma en groupe affine représenté par A alors il existe une correspondance entre les représentation de E sur le module V et les comodule de la forme $\rho : V \longrightarrow V \otimes A$.*

Démonstration Nous allons nous inspirer du la preuve de lemme de Yoneda. Soit $\psi : E \longrightarrow GL_V$ une représentation. On pose $\rho = \psi(id_A)|V$. Si $g : A \longrightarrow B$ est un morphisme d'algébres alors en restreignant $V \otimes A$ et $V \otimes R$ à V, on obtient le diagramme commutatif :



Donc $\psi(g) = (id \otimes g) \circ \rho$. Ensuite on utilise le fait que $\psi(e) = 1$, $\psi(gh) = \psi(g)\psi(h)$ pour tous $g, h \in E(A)$ et la relation précédente, on tire les axiomes de comodule pour ρ.

Lemme 7 *Supposons que B soit un corps. Si $v_1, ..., v_n$ est une base de V alors pour toute algébre R sur B les vecteurs $v_1 \otimes 1_R, ..., v_n \otimes 1_R$ forment une famille libre sur R.*

Démonstration Soient $a_1, a_2, ..., a_n$ des éléments de R et (e_α) une base sur B de R. Supposons que

$$v_1 \otimes a_1 + v_2 \otimes a_2 + ... + v_n \otimes a_n = 0$$

Posons $a_i = \sum_\alpha b_{\alpha,i} e_\alpha$ pour $i = 1, ..., n$. En remplaçant, il vient :

$$\sum_{i=1}^{n} \sum_{\alpha} b_{\alpha,i} v_i \otimes e_\alpha = 0$$

Enfin, les $v_i \otimes e_\alpha$ forment une famille libre sur B. Donc $b_{\alpha,i} = 0$ pour tous i, α. Donc $a_i = 0$ pour $i = 1, 2, ..., n$, ce qui montre notre résultat.

Lemme 8 *Supposons que B soit un corps. Soient $v_1, v_2, ..., v_n$ des vecteurs de base de V et $\rho : V \longrightarrow V \otimes A$ un comodule. Si $\rho(v_i) = \sum_\alpha v_i \otimes a_{i,j}$ alors $M(a_{i,j}) = \sum_k a_{i,k} \otimes a_{k,j}$ pour $i, j = 1, ..., n$.*

Démonstration De la relation : $(\rho \otimes id) \circ \rho = (id \otimes M) \circ \rho$, on obtient :

$$(id \otimes M)\rho(v_j) = \sum_{i=1}^{n} v_i \otimes M(a_{i,j}) = \sum_{i=1}^{n} v_i \otimes \sum_{k=1}^{n} a_{i,k} \otimes a_{k,j}$$

pour tout $j = 1, 2, ..., n$. Ensuite, on retranche et on utilise le fait que $v_1 \otimes 1_{A\otimes A}$,...,$v_n \otimes 1_{A\otimes A}$ est une famille libre de $A \otimes A$ par le lemme précédent.

Lemme 9 *Supposons que B soit un corps. Soit $\rho : T \longrightarrow T \otimes A$ un comodule sur B. Alors tout vecteur v de T appartient à un sous-comodule W de dimension finie sur B.*

Démonstration Soit (a_α) une base de A. Ecrivons

$$v = \sum_\alpha v_\alpha \otimes a_\alpha = \sum_{\alpha \in Z} v_\alpha \otimes a_\alpha$$

avec Z un ensemble fini. Alors nous affirmons que l'espace vectoriel W engendré par la famille $\{v_\alpha | \alpha \in Z\}$ convient. En effet, en utilisant $(id \otimes M)\rho = (\rho \otimes id)\rho$, il vient :

$$\sum_\gamma \rho(v_\gamma) \otimes a_\gamma = \sum_{\alpha \in Z} \sum_{\beta,\gamma} v_\alpha \otimes s_{\alpha,\beta,\gamma} a_\beta \otimes a_\gamma$$

avec

$$M(a_\alpha) = \sum_{\beta,\gamma} s_{\alpha,\beta,\gamma} a_\beta \otimes a_\gamma$$

Puis, en comparant les deux décompositions :

$$\rho(v_\gamma) = \sum_{\alpha \in Z} \sum_{\beta,\gamma} v_\alpha \otimes s_{\alpha,\beta,\gamma} a_\beta$$

Donc $\rho(W) \subset W$.

Définition Soient E, F deux schémas en groupe affines de même base représenté respectivement par les algébres de Hopf A et B. On dit que E est un sous-groupe fermé de F s'il existe un morphisme surjectif B vers A.

Notons que dans la définition précédente, si E et F sont représentés par $Spec(A)$ et $Spec(B)$ alors $Spec(A)$ est un sous-schéma fermé de $Spec(B)$. Par ailleurs, nous appelons schéma en groupe algébrique sur B tout schéma en groupe affine représenté par une algébre de Hopf de type fini sur B. Les lemmes précédents aboutissent au résultat remarquable :

Théorème 5 *Tout schéma en groupe algébrique sur un corps est sous-groupe fermé d'un certain GL_n.*

Démonstration Supposons que B soit un corps. Soient E un schéma en groupe algébre représenté par une algébre de Hopf $A = B[x_1, x_2, ..., x_m]$ vu comme comodule. Par le lemme précédent chaque x_i est dans un sous-comodule de dimension W_i de dimension finie sur B. Notons

$$W = W_1 \oplus W_2 \oplus ...W_m$$

C'est un sous-comodule de dimension finie. Soient alors $v_1, v_2, ..., v_n$ des vecteurs de base de V,

$$M(v_j) = \sum_{i=1}^{n} v_i \otimes a_{i,j}$$

et $X = (X_{i,j})$ pour tout entier $i, j = 1, ..., n$. Donc le morphisme

$$\psi : B[X, \det(X)^{-1}] \longrightarrow A$$

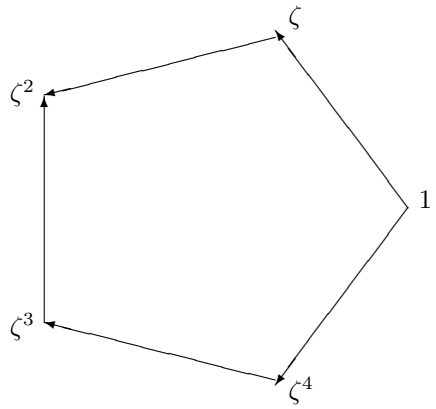
qui à X associe $(a_{i,j})$ est un morphisme d'algébre de Hopf puisque $M(a_{ij}) = \sum_{k=1}^{n} a_{i,k} \otimes a_{k,j}$ pour tous i, j. En outre, l'image de ψ contient W et donc les générateurs de A. Donc ψ est surjectif.

1.2.5 Le schéma en groupe μ_n

Soient B un anneau, n un entier ≥ 0 et G un groupe abélien. G est noté additivement.

Pour toute algébre R sur B, on note $\mu_n(R)$ le groupe des éléments de R solution du polynôme $X^n - 1$. Si $\psi : R \longrightarrow S$ est un morphisme d'algébres alors pour tout $a \in \mu_n(R)$, $\psi(a)^n = \psi(a^n) = 1$, ce qui définit un morphisme naturel $\mu_n(R) \longrightarrow \mu_n(S)$. Par suite, μ_n est un schéma affine représenté par $Hom(B[X]/(X^n - 1), R) = \mu_n$.

Le dessin ci-dessous représente μ_5 sur les complexes :



Définition On note $B[G]$ l'algébre sur B définie comme le module libre :

$$\bigoplus_{\alpha \in G} Be_\alpha$$

muni du produit $e_\alpha e_\beta = e_{\alpha+\beta}$ sur pour tous $\alpha, \beta \in G$ sur les vecteurs de base $(e_\alpha)_{\alpha \in G}$.

On définit une structure d'algébre de Hopf sur $B[G]$ en posant $M(e_\alpha) = e_\alpha \otimes e_\alpha$, $\varepsilon(e_\alpha) = 1$ et $I(e_\alpha) = e_{-\alpha}$ pour tout $\alpha \in M$.

Définition Un schéma en groupe affine est dit diagonalisable s'il est représenté par une algébre de Hopf de la forme $B[G]$.

Proposition 29 *μ_n et G_m sont diagonalisables.*

Démonstration Tout d'abord, on a les isomorphismes d'algébres :

$$\psi_1 : B[X]/(X^n - 1) \longrightarrow B[\mathbb{Z}/n\mathbb{Z}]$$

$$\psi_2 : B[X, \frac{1}{X}] \longrightarrow B[\mathbb{Z}]$$

qui tous deux envoie la classe de X sur e_1. Après :

$$\psi_1 \circ M(X^p) = \psi_1(X^p \otimes X^p) = e_p \otimes e_p = M(e_p)$$

pour $1 \geq p \geq n$. Ce qui montre que ψ_1 est un isomorphisme d'algébres de Hopf. Pour ψ_2, le reaisonnement est analogue.

Lemme 10 *Si G_1 et G_2 sont deux groupes albéliens alors on a l'isomorphisme d'algébres de Hopf :*

$$B[G_1 \oplus G_2] \longrightarrow B[G_1] \otimes B[G_2]$$

Démonstration Le morphisme d'algébres

$$\psi : \bigoplus_{(\alpha,\beta) \in G_1 \oplus G_2} Be_{(\alpha,\beta)} \ni e_{(\alpha,\beta)} \mapsto e_\alpha \otimes e_\beta \in \bigoplus_{(\alpha,\beta) \in G_1 \oplus G_2} Be_\alpha \otimes e_\beta$$

envoie une base sur une autre, c'est donc un isomorphisme. Enfin, on conclut par :

$$\psi \circ M(e_{(\alpha,\beta)}) = M(e_\alpha \otimes e_\beta)$$

Notation Soit A une algébre de Hopf sur B. On note $\chi(A)$ le groupe des éléments $a \in A$ tels que $M(a) = a \otimes a$.

On aura remarqué que si $A = B[G]$ alors tous les éléments $(e_\alpha, \alpha \in G)$ sont exactement les élément de $\chi(A)$.

Proposition 30 *Supposons que B soit un corps. Si A est une algébre de Hopf alors $\chi(A)$ est une famille linéairement indépendante sur B.*

Démonstration Puisque l'anneau de base est un corps, il existe une sous-famille non vide maximale T de $\chi(A)$. Supposons par contradiction qu'il existe $a \in \chi(A)$ tel que $a \notin T$. Donc a appartient au sous-espace vectoriel engendré par T, ce qui s'ecrit : $a = \sum_i \lambda_i \zeta_i$ avec $\zeta_i \in \chi(A)$. Donc :

$$1 = \varepsilon(a) = \sum_i \lambda_i$$

$$\sum_{i,j} \lambda_i \lambda_j \zeta_i \oplus \zeta_j = M(a) = \sum_i \lambda_i M(a_i) = \sum_i \lambda_i \zeta_i \oplus \lambda_i$$

Donc $\lambda_i \lambda_j = \delta_{i,j} \lambda_i$. Donc $\lambda_i \in \{0, 1\}$ et comme $\sum_i \lambda_i = 1$, on déduit que seulement un seul λ_i est égal à 1. Donc $a \in T$, ce qui donne notre contradiction.

Lemme 11 *Si B est un corps alors la catégorie des groupes abéliens est anti-équivalente à celle des schémas en groupe diagonalisable.*

Démonstration Soit R foncteur qui à tout groupe abélien T associe l'algébre de Hopf $B[T]$ des schémas en groupe diagonalisable. Montrons que son inverse est donné par la règle $S : A \longmapsto \chi(A)$. Soit T un groupe abélien. Donc $S \circ R(T) = \chi(B[T])$. Notons encore T les éléments e_α avec $\alpha \in T$. Donc $T \subset \chi(B[T])$. Donc par le lemme précédent et comme est T est une base de $B[T]$ on a $\chi(B[T]) = T$. Ensuite par un argument analogue si $A = B[T]$ alors $T = \chi(A)$ et $R \circ S(A) = A$. Enfin, si A' est une algébre représentant un schéma en groupe diagonalisable alors on a directement $Hom(A, A') \cong Hom(B[\chi(A')], B[\chi(A)])$.

Théorème 6 *Supposons que B soit un corps. Tout schéma en groupe affine diagonalisable d'algébre de Hopf A de type fini sur B s'ecrit de manière unique à permutation des facteurs près comme produit*

$$\prod_{i=1}^{k} G_m \times \prod_{i=1}^{l} \mu_{d_i}$$

avec $d_1|d_2|...|d_{l-1}|d_l$.

Démonstration Par hypothèse, il existe $x_1, x_2, ..., x_n \in B$ tels que $A = B[x_1, x_2, ..., x_n]$. Pour tout $i = 1, 2, ...n$ écrivons $A = B[G]$ avec G un groupe abélien, $x_i = \sum_{\alpha \in Z_i} a_{\alpha,i} e_\alpha$ avec $Z_i \subset G$ en partie finie,

$$U = \{e_\alpha | \alpha \in \cup_{i=1}^{n} Z_i\}$$

et G' le sous-groupe engendré par l'ensemble fini U. Donc puisque $B[G] = B[G']$, on a $G' = G$. Donc G est de type fini sur $\mathbb{Z}$ et s'ecrit comme produit

$$\bigoplus_{i=1}^{k} \mathbb{Z} \oplus \bigoplus_{i=1}^{l} \mathbb{Z}/d_i\mathbb{Z}$$

avec $d_1|d_2|...|d_n$. L'unicité provient du lemme précédent.

Définition Soit E un schéma en groupe affine représenté par une algébre de Hopf libre A de dimension fini. On appelle ordre de E la dimension A.

Corollaire 4 *Tout schéma en groupe diagonalisable d'ordre fini sur un corps a pour ordre le nombre d'éléments de son groupe abélien correspondant.*

Démonstration Supposons que B soit un corps. Si E est un schéma en groupe diagonalisable représneté par $A = B[G]$ une algébre de dimension finie alors notons $o(E)$ son ordre et $E \cong \prod_{i=1}^{l} \mu_{d_i}$ pour des entiers $d_1|d_2|...|d_l$. Donc

$$o(E) = dim(A) = dim(\bigotimes_{i=1}^{l} B[X]/(X^{d_i} - 1)) = \prod_{i=1}^{l} d_i$$

qui est le cardinal de G.

Définition Soit T un groupe fini abélien ou non. On considère l'algébre de Hopf

$$B^T = \bigoplus_{\alpha \in T} Be_\alpha$$

avec les régles :

(GC1)

$$e_\alpha e_\beta = \delta_{\alpha,\beta} e_\alpha$$

(GC2)

$$\sum_{\alpha \in T} e_\alpha = 1$$

(GC3)

$$M(e_\alpha) = \sum_{\alpha=\beta\gamma} e_\beta \otimes e_\gamma$$

pour tous $\alpha, \beta \in T$. Le schéma en groupe affine associé à l'algébre B^T est appelé constant et lorsqu'il n'y a pas d'ambiguïtés, on le dénote par T.

La proposition suivante est à titre d'exemple :

Proposition 31 *Si* 2 *est un élément inversible dans* B *alors* $\mathbb{Z}/2\mathbb{Z}$ *et* μ_2 *sont isomorphes.*

Démonstration On considère le morphisme d'algébres

$$\phi : B[X]/(X^2-1) \longrightarrow B^2$$

qui à la classe de X associe $(1,-1)$. Désignons par X la classe de X et par a, b des éléments de B. Si $\phi(bX+a) = 0$ alors $(a+b, a-b) = 0$ et donc $a = b = 0$ puisque 2 est inversible. Donc ϕ est injectif. De même si $(c,d) \in B^2$ alors $\phi(\frac{c-d}{2}X + \frac{c+d}{2}) = (c,d)$. Donc ϕ est un isomorphisme. Enfin, ϕ préserve la comultiplication :

$$\phi \circ M(bX+a) = (a+b, a-b) \otimes (a+b, a-b) = M \circ \phi(bX+a)$$

nous nous plaçons dans le contexte des modules projectifs, pour plus de détails voir l'appendice à ce sujet.

Définition Un schéma en groupe affine représenté par une algébre V est dit fini si V est un module projectif de type fini.

Soit E un schéma en groupe affine abélien fini représenté par une algébre V. On considère la multiplication $m : V \otimes V \longrightarrow V$ qui à tout tenseur élémentaire $a \otimes b$ associe ab, l'application coinverse $I : V \longrightarrow V$ et le morphisme $j : B \longrightarrow V$ munissant V d'une struture d'algébre. En dualisant ces morphismes, il s'ensuit :

Théorème 7 V^* *munie de* m^*, I^* *et* j^* *est une algébre de Hopf pour la multiplication* M^* *et représente un schéma en groupe affine que l'on dénote par* E^*. *Si* F *est un schéma en groupe affine abélien fini alors* $Hom(E,F) \cong Hom(F^*, E^*)$

Démonstration Supposons que F soit représenté par W et $\phi : V \longrightarrow W$ soit un morphisme d'algébres sur B. Donc $\phi \circ m = m \circ \phi \otimes \phi$. Donc en dualisant : $m^* \circ \phi^* = (\phi \otimes \phi)^* \circ m^*$ et puisque les morphismes $(\phi^*)^*$ s'identifie naturellement aux morphismes ϕ, on déduit que l'on a un isomorphisme naturel entre les morphismes V vers W d'algébres et les morphismes de W^* vers V^* préservant m^*. Ce dernier point montre que m^* et M^* sont respectivement coassociative et associative. En effet, il suffit de dualiser les diagrammes d'associativité et de coassociativité de m et M. De même, la multiplication M^* préserve m^* en remplaçant dans le raisonnement précédent ϕ par m. Il reste à montrer que I^* est bien un morphisme préservant M^*. Mais cela est équivalent à $M \circ I = (I \otimes I) \circ M$ qui est vrai puisque E est un schéma en groupe affine abélien.

Proposition 32 *Les schémas en groupes affines* $\mathbb{Z}/n\mathbb{Z}^*$ *et* μ_n *sont isomorphes.*

Démonstration Soient k, l, α des éléments de $\mathbb{Z}/n\mathbb{Z}$. Pour alléger les notations, notons $(e_0, e_1, ...e_{n-1})$ la base duale de la base canonique. On vérifie que :

$$M^*(e_k \otimes e_l)(e_\alpha) = \sum_{\alpha=\beta+\gamma} \delta_{\beta,k}\delta_{\gamma,l}$$

Si $\alpha = k+l$ alors $M^*(e_k \otimes e_l)(e_\alpha) = 1$. Si $\alpha \neq k+l$ alors dans la somme ci-dessus si $\beta \neq k$ alors $\gamma \neq l$ car sinon on aurait $\alpha = k+l$, donc $M^*(e_k \otimes e_l)(e_\alpha) = 0$. Le raisonnement est analogue pour $\gamma = l$ et le dernier cas $(\gamma, \beta \neq 0)$ donne encore 0. Donc le produit de e_k par e_l donne e_{k+l}. Donc on a un morphisme d'algébres :

$$\phi : (B^n)^* \longrightarrow B[X]/(X^n - 1)$$

qui à la classe de X associe e_1. C'est un isomorphisme puisque qu'il envoie une base sur une base. En outre, ϕ préserve les comultiplications :

$$\phi \otimes \phi \circ (m^*(e_l)) = \phi \otimes \phi(e_l \otimes e_l) = X^l \otimes X^l = \mu(X^l) = \mu \circ \phi$$

où μ désigne la comultiplication de μ_n.

Le résultat ci-dessus se généralise directement :

Corollaire 5 *Supposons que B soit un corps. Le passage au dual donne une anti-équivalence de catégories entre les schémas en groupe constants et les schémas en groupe diagonalisables. Par conséquent, la catégorie des schémas en groupe constants est équivalente à celle des groupes abéliens finis.*

1.2.6 Produits semi-directs de schémas en groupe affine

Nous rappelons la notion de produit direct de groupes abéliens. On note par la lettre e l'élément neutre de tout groupe concerné.

Soient H et K deux groupes. Nous allons montrer que l'on peut trouver un groupe G tel que la suite :

$$\{e\} \longrightarrow H \longrightarrow G \longrightarrow K \longrightarrow \{e\}$$

soit exacte. La définition suivante répond à ce problème.

Définition Le produit semi-direct de H par K selon le morphisme $\psi : K \longrightarrow Aut(H)$ à valeur dans les automorphismes de groupe de K est l'ensemble $H \times K$ muni de la multiplication :

$$g_1.g_2 = (h_1\psi(k_1)(h_2), k_1k_2)$$

avec $g_1 = (h_1, k_1)$ et $g_2 = (h_2, k_2)$ des éléments de $H \times K$.

Vérification La vérification de l'associativité est laissée aux lecteurs. L'inverse de $(h,k) \in H \times K$ est donné par :

$$(\psi(k^{-1})(h^{-1}), k^{-1})$$

et l'élément neutre est (e,e). Donc G est un groupe. En outre si $(u,v) \in G$ alors :

$$(u,v)(h,e)(u,v)^{-1} = (u\psi(v)(h)u^{-1}, e) \in H \times \{e\}$$

Donc $H \times \{e\}$ est un sous-groupe distingué. Une autre manière de le voir est de considérer la projection naturelle $p : G \longrightarrow K$ qui est un morphisme de groupes surjectif de noyau $H \times \{e\}$. Ainsi $G/H \times \{e\} \cong K$. Enfin $H \times \{e\}$ est isomorphe à H puisque :

$$(h,e)(u,e) = (h\psi(e)(u), e) = (hu, e)$$

Notons qu'en général K n'est pas distingué dans G.

Lorsqu'il n'y a pas d'ambiguïté, on note $H \ltimes K$ le produit semi-direct de H par K. Pour une partie $Z \subset G$, on note $< Z >$ le sous-groupe engendré par Z.

Proposition 33 *Soient G un groupe et H, K des sous-groupes. G est isomorphe à $H \ltimes K$ si et seulement si H est distingué dans G, $< HK >= G$ et $H \cap K = \{e\}$.*

Démonstration Pour le sens direct, on se place dans le cas $G = H \ltimes K$ en identifiant respectivement H et K par $H \times \{e\}$ et $\{e\} \times K$. Inversement, notons $(h,k), (u,v) \in H \times K$, $\psi : K \longrightarrow Aut(H)$ le morphisme défini par $\psi(k)(h) = khk^{-1}$, $H \ltimes K$ le produit semi-direct selon ψ et $p : H \ltimes K \longrightarrow < HK >$ l'application qui à (h,k) associe hk. Donc

$$p((h,k)(u,v)) = h\psi(k)(u)kv = hkuv = p(h,k)p(u,v)$$

Tout élément de $< HK >$ s'ecrit comme produit d'un élément de H par un élément de K. En effet, on raisonne par recurrence sur la longueur l des mots. Si $l \leq 2$ alors l'affirmation est vrai. Supposons que cette dernière est vraie pour $l + 1 = 2p + 1 > 2$ fixé. Notons :

$$\prod_{i=1}^{p} h_i k_i = h_1 k_1 h_2 k_2 ... h_{p-1} e(k_{p-1} h_p k_p) = \mu(k_{p-1} h_p k_p)$$

avec $(h_i, h_i) \in H \ltimes K$. Donc on applique l'hypothèse de récurrence à μ. Ensuite

$$k_{p-1} h_p k_p = (k_{p-1} h_p k_{p-1}^{-1}) k_{p-1} k_p$$

s'ecrit comme produit d'un élément de H par un élément de K. Aprés, on applique à nouveau l'hypothèse de récurrence à la concaténation. Pour le cas l impair, on rajoute l'élément neutre. Ceci nous montre que p est surjectif. Enfin $Ker(p) = \{e\}$ puisque $H \cap K = \{e\}$ et on a un isomorphisme.

Pour n un entier ≥ 1, notons C_n le groupe $\mathbb{Z}/n\mathbb{Z}$ noté multiplicativement et G_n le groupe libre à n générateurs.

Définition Le groupe diédral D_n est le groupe G_2 engendré par les lettres σ et τ sous les contraintes : $\sigma^2 = e$, $\tau^n = e$ et $\sigma\tau = \tau^{-1}\sigma$.

Proposition 34 *D_n est produit semi-direct de C_n par C_2.*

Démonstration On remarque le groupe H engendré par τ est d'indice 2 dans D_n donc H est distingé dans D_n. Ensuite si l'on note K le sous-groupe engendré par σ alors $H \cap K = \{e\}$. Enfin par la relation $\sigma\tau = \tau^{-1}\sigma$, on a $HK = D_n$. Puisque H et K sont isomorphes respectivement à C_n et C_2, on obtient le résultat par la propositon précédente.

Revenons maintenant à la théorie des schémas en groupe affines.

Définition Soit E un schéma en groupe affine. Une immersion férmée F de E est dite normale si pour toute algébre R sur B, $F(R)$ est un sous-groupe distingué de $E(R)$.

Soient E un schéma en groupe affine et F, G deux immersions fermées de E tel que F soit normale. Les résultats précédents sur les produits semi-directs inspirent la définition suivante :

Définition On dit que E est produit semi-direct de F et G si la multiplication :

$$F(R) \times G(R) \longrightarrow E(R)$$

est bijective pour toute algébre R sur B.

Définition Soit $\psi : E \longrightarrow E'$ un morphisme de schémas en groupe affines. On appelle noyau de ψ noté $Ker(\psi)$ le foncteur de groupes défini par $Ker(\psi)(R) = Ker(\psi(R))$ pour toute algébre R sur B.

Proposition 35 *Si $\psi : E \longrightarrow E'$ est un morphisme entre schémas en groupe affines alors $Ker(\psi)$ est une immersion fermée de E.*

Démonstration Supposons que E et E' soient représentés par R et S. Alors $Ker(\psi)$ est le produit fibré des morphismes ψ et $\{e\} \longrightarrow E'$ que l'on note $E \times_{E'} \{e\}$. Donc $Ker(\psi)$ est un schéma en groupe affine représenté par $R \otimes_S B$. Les structures d'algébres sur S étant donné par le morphisme $s : S \longrightarrow R$ induit par ψ et l'augmentation $\varepsilon : S \longrightarrow B$. Notons I le noyau ε. Donc le morphisme naturel surjectif $R \longrightarrow R \otimes_S B$ donne un isomorphisme entre R/IR et $R \otimes_S B$. Enfin, on transporte la comultiplication de $R \otimes_S B$ sur R/IR afin de munir cette dernière d'un structure d'algébre de Hopf.

La proposition suivante nous sera fort utile beaucoup plus tard :

Proposition 36 *E est produit semi-direct de F et G si et seulement si il existe un morphisme $\psi : E \longrightarrow G$ dont sa restriction sur G est l'identité et dont le noyau est F.*

Démonstration Soit R une algèbre sur B. Donc la multiplication :

$$F(R) \times G(R) \longrightarrow E(R)$$

est bijective. Ce qui équivaut à : $F(R) \cap G(R) = \{e\}$ et $E(R) = F(R)G(R)$. Donc $E(R) = F(R) \ltimes G(R)$. Donc par un argument précédent la projection naturelle $p(R) : E(R) \longrightarrow G(R)$ est de noyau $F(R)$. Inversement, soit $\psi : E \longrightarrow G$ un morphisme verifiant : $Ker(\psi) = F$ et $\psi | G = id_G$. Soit $a \in E(R)$. La décomposition $a = a\psi(a^{-1})\psi(a)$ montre que $E(R) = F(R)G(R)$. Soit $b \in F(R) \cap G(R)$ et l'intersection de $F(R)$ et $G(R)$ est réduite à $\{e\}$ puisque si $b \in G(R) \cap F(R)$ alors $b = \psi(b) = e$. D'où le résultat.

Donnons maintenant un exemple :

Soient p un nombre premier et K un corps de caractéristique p. On considère l'algébre de Hopf $A = K[X, Y]/(X^p - 1, Y^p)$ de comultiplication :

$$M(X, Y) = (X \otimes X, Y \otimes 1 + X \otimes Y)$$

On dénote par E le schéma en groupe affine associé. Si R est une algébre sur K alors $E(R)$ est en fait le groupe des matrices de type $(2, 2)$:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

avec $a \in \mu_p(R)$ et $b \in \alpha_p(R)$.

Proposition 37 *Le schéma en groupe affine E comme ci-dessus est produit semi-direct de α_p par μ_p.*

Démonstration Soient R une algébre sur K et M une matrice de $E(R)$. Donc on écrit :

$$M(a, b) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = T(b)U(a)$$

avec $a \in \mu_p(R)$ et $b \in \alpha_p(R)$. On observe que les éléments de la forme $T(b)$ et $U(a)$ forment respectivement des groupes isomorphes $\alpha_p(R)$ et μ_p. Soit maintenant $\psi : E \longrightarrow \alpha_p$ le morphisme de schéma en groupe affine qui à toute matrice $M(a, b)$ associe $T(b)$. Enfin, on a le résultat puisque : $\psi | \alpha_p = id_{\alpha_p}$ et $Ker(\psi) = \mu_p$.

1.2.7 Schémas en groupe affines d'ordre 2

Nous allons décrire les schémas en groupe affines d'ordre 2 sur un anneau principal intègre. Pour cela nous considérons un anneau principal B et A une algébre de Hopf qui soit un module libre sur B de rang 2. On note comme d'habitude $\varepsilon : A \longrightarrow B$ l'augmentation de noyau I et M la comultiplication.

Lemme 12 *A est somme directe de I et B.*

Démonstration Soit x un élément de $I \cap B$. Alors :

$$x = x\varepsilon(1) = \varepsilon(x) = 0$$

Ensuite, comme ε est l'identité sur B, si $w \in A$ alors on a la décomposition :

$$x = (x - \varepsilon(x)) + \varepsilon(x) \in A + B$$

Proposition 38 *Tout élément x de I vérifie la congruence :*

$$M(x) \equiv x \otimes 1 + 1 \otimes x$$

modulo $I \otimes I$.

Démonstration Notons $f(x) = M(x) - 1 \otimes x - x \otimes 1$ et $M(x) = \sum_\alpha x_\alpha \otimes y_\alpha$. Donc :

$$(\varepsilon \otimes id) \circ f(x) = \sum_\alpha \varepsilon(x_\alpha) \otimes y_\alpha - 1 \otimes x = 1 \otimes (\sum_\alpha \varepsilon(x_\alpha) y_\alpha - x) = 0$$

De même, $(\varepsilon \otimes \varepsilon) \circ f = (id \otimes \varepsilon) \circ f = 0$. Notons J l'intersection des noyaux de $\varepsilon \otimes \varepsilon$, $\varepsilon \otimes id$ et $id \otimes \varepsilon$. Soient u, v les vecteurs de base de A et considérons :

$$z = \lambda_1 u \otimes u + \lambda_2 u \otimes v + \lambda_3 v \otimes u + \lambda_4 v \otimes v$$

un élément de J. Donc en appliquant $id \circ \varepsilon$, on déduit $\lambda_1 x + \lambda_2 y$, $\lambda_3 x + \lambda_4 y$ appartient à I. Donc $z \in A \otimes I$. Similairement, en faisant le raisonnement avec $\varepsilon \circ id$, on a $z \in I \otimes A$. Par la théorie des module de type fini sur un anneau principal, il existe $d \in B$ tel que disons (du) soit une base de B. Donc $(u \otimes du, v \otimes du), (du \otimes u, du \otimes v)$ sont respectivement des bases de $A \otimes I$ et $I \otimes A$. Donc en décomposant z dans ces deux bases, on en déduit que z est un multiple de $du \otimes u$. Or par intégrité de B, $\varepsilon(du) = 0$ implique $\varepsilon(u) = 0$. Donc $u \in I$. Donc $z \in I \otimes I$. D'où le résultat.

En particulier, en posant $w = du$, il existe $b \in B$ tel que

$$M(w) = w \otimes 1 + 1 \otimes w + bw \otimes w$$

Lemme 13 *Si X est une indéterminée alors il existe un élément $a \in B$ tel que A soit isomorphe à $B[X]/(X^2 + aX)$. En outre, si $I = wB$ et si $M(w) = w \otimes 1 + 1 \otimes w + bw \otimes w$ alors on a l'identité : $(2 - ab)^2 = 2 - ab$.*

Démonstration Avec les mêmes notations que précédemment, $w^2 \in I = wB$. Donc il existe $a \in B$ tel que $w^2 + aw = 0$. Cette égalité est non triviale, i.e $a \neq w$ puisque dans le cas contraire, cela implique $w = 0$. Ensuite $A = B[w]$. Considérons le morphisme :

$$\psi : A = B[X] \longrightarrow B[w]$$

qui à X associe w. Donc $(X^2 + a) \subset Ker(\psi)$. Soit $P \in Ker(psi)$. Comme $X^2 + aX$ est unitaire, il existe un polynôme $S \in B[X]$ et $a_0, a_1 \in B$ tels que :

$$P = S(X^2 + aX) + a_1X + a_0$$

En appliquant ψ, il vient $a_1w + a_0 = 0$. Or a_0 est nul puisque $a_0 = -a_1w \in B \cap I$. Aprés, $a_1 = 0$ puisque (w) est libre. Donc $P \in (X^2 + aX)$ et ψ se factorise en l'isomorphisme voulu. La deuxième affirmation provient du calcul $M(w^2) - M(w)^2 = 0$ et en appliquant : $w^2 = -aw$.

Lemme 14 *Avec les mêmes notations que précédemment, on a : $ab = 2$.*

Démonstration Notons S le morphisme coinverse de A. S est un automorphisme linéaire de A vérifiant $S \circ S = id$. De ce fait $S(w) \in I$ et donc il existe $u \in B$ tel que $S(w) = uw$. Ainsi l'identité :

$$w = S \circ S(w) = u^2w$$

donne $u = \pm 1$. Montrons que dans tous les cas on a $S(w) = w$. En effet, si $S(w) = -w$ alors :

$$0 = (id, S) \circ M(w) = bw^2 = -abw$$

Donc $ab = 0$ et par l'identité $(2 - ab)^2 = (2 - ab)$, on $2 = 0$. Ce qui donne $S(w) = -w = w$. Donc ayant $S(w) = w$, il vient :

$$0 = (id, S) \circ M(w) = (2 - ab)w$$

D'où $2 = ab$.

La vérification suivante est laissée aux lecteurs :

Lemme 15 *Si a, b sont des éléments de B tels que $ab = 2$ alors $R = B[X]/(X^2 + a)$ muni du morphisme $M : R \longrightarrow R \times R$ défini par :*

$$M(w) = w \otimes 1 + 1 \otimes w + bw$$

est une algébre de Hopf.

On note $E_{a,b}$ le schéma en groupe affine représenté par l'algébre R comme ci-dessus. Les lemmes précédents mis bout à bout nous donnent :

Théorème 8 *Tout schéma en groupe affine d'ordre 2 est isomorphe à un $E_{a,b}$ avec $a, b \in B$ tels que $ab = 2$*

Par une vérification standard on a :

Lemme 16 *Soient a, b, c, d des éléments de B tels que $ab = cd = 2$. $E_{a,b}$ et $E_{c,d}$ sont isomorphes si et seulement si il existe un élément inversible u de B tel que $a = uc$ et $b = u^{-1}d$.*

Il y a donc deux possibilités lorsque $B = \mathbb{Z}$ ...

Théorème 9 *Les seuls schémas en groupe affines d'ordre 2 sur $\mathbb{Z}$ sont μ_2 et $\mathbb{Z}/2\mathbb{Z}$.*

et une seule lorsque B est un corps de caractéristique impaire ou nulle.

Théorème 10 *Tout schéma en groupe affine d'ordre 2 sur un corps de caractristique impaire ou nulle est isomorphe à μ_2.*

2 Groupe versus Schéma en groupe affine

2.1 Schéma en groupe affine fini et étale

2.1.1 Idempotents et connexité

Soit S un anneau.

Si X est un espace toplogique, nous rappelons que X est connexe s'il ne peut pas s'ecrire comme union disjointe de deux fermés non triviaux. Dans ce paragraphe nous étudions les composantes connexes des schémas affines :

Définition Un élément $e \in S$ est dit idemptotent si $e^2 = e$.

On a ainsi directement le résultat :

Proposition 39 *Soit e un élément idempotent de S alors S est le produit direct des anneaux eS et $(1-e)S$.*

Ce qui se traduit en terme de schémas affines par :

Lemme 17 *Soit e un élément idempotent de S alors $Spec(S)$ est union disjointe des fermés $V(e)$ et $V(1-e)$.*

Démonstration Si $\mathfrak{a}$ est un idéal contenant e et $1-e$ alors $1 = e + 1 - e \in \mathfrak{a}$. Ainsi $\mathfrak{a}$ ne peut pas être premier et donc $V(e) \cap V(1-e)$ est vide. Ensuite :

$$V(e) \cup V(1-e) = V(e(1-e)) = Spec(S)$$

Corollaire 6 *$Spec(S)$ est connexe si et seulement si S ne possède pas d'éléments idempotents autres que 1 et 0.*

Lemme 18 *Deux éléments idempotents e, f de S sont égaux si et seulement si $V(e) = V(f)$.*

Démonstration Si $V(e) = V(f)$ alors par ce qui précéde :

$$Spec(S) = V(e) \cup V(1-e) = V(f) \cup V(1-e) = V(f(1-e))$$

Donc il existe un entier N positif tel que $f^N(1-e)^N = 0$. Mais cela implique $f(1-e) = 0$ puisque $f(1-e)$ est idempotent. Donc $f = fe$. En faisant le raisonnement dans l'autre sens, on obtient $e = fe$. D'où $e = f$.

Théorème 11 *Les éléments idempotents de S correspondent bijectivement aux composantes connexes de $Spec(S)$*

Démonstration Par les lemmes précédents, on a montré que l'application

$$e \longmapsto V(e)$$

de l'ensemble des idempotents vers les composantes connexes de $Spec(S)$ était injectif. Il reste à montrer la surjectivité. Soit $V(\mathfrak{a})$ une composante connexe. Alors il existe un idéal $\mathfrak{b}$ tel que $V(\mathfrak{a}) \cup V(\mathfrak{b}) = Spec(S)$ et $V(\mathfrak{a}) \cap V(\mathfrak{b}) = \emptyset$. Donc il existe $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ tels que $a + b = 1$ et $(ab)^N = 0$ pour un certain enteir positif N. Après, puisque aucun idéal maximal contient à la fois a^N et b^n, il existe $u, v \in \mathfrak{ab}$ tel que $ua^N + vb^N = 1$. Enfin, $V(\mathfrak{a}) = V(e)$ avec $e = ua^N$ qui est idempotent.

Proposition 40 *Si S est un anneau noethérien alors il ne posséde qu'un nombre fini d'idempotents.*

Démonstration En effet, si A possède une infinité d'idempotents alors par le théorème précédent on peut trouver une suites strictement décroissante de composantes connexes :

$$Spec(S) = V(\mathfrak{a}_1) \supset V(\mathfrak{a}_2) \supset ... \supset V(\mathfrak{a}_k) \supset V(\mathfrak{a}_{k+1}) \supset ...$$

Ce qui nous donne suite d'ideaux stricte :

$$\sqrt{(0)} = \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset ... \subset \mathfrak{a}_m \subset ...$$

On a donc notre contradiction.

Donnons des exemples :

Proposition 41 *Si X est une indéterminée alors $Spec(\mathbb{R}[X]/X^n - 1)$ n'est pas un espace topologique connexe pour tout entier $n > 1$.*

Démonstration Tout d'abord, remarquons que :

$$X^n - 1 = (X - 1)(1 + X + X^2 + ... + X^{n-1}) = (X - 1)T$$

et que $X^n - 1$ dans $\mathbb{C}$ est scindé à racines simples. Donc $(X - 1)$ et T n'ont pas de racines communes sur $\mathbb{C}$. Or puisque $\mathbb{R}[X]$ est principal, il existe un polynôme $D \in \mathbb{R}[X]$ tel que $(D) = (X - 1, T)$. Donc D divise à la fois $X - 1$ et T, ce qui force par les remarques précédentes : D inversible. Donc $X - 1$ et T sont permiers entre eux et par le théorème Chinois, on a l'isomorphisme :

$$\psi : A = \mathbb{R}[X]/(X - 1) \times \mathbb{R}[X]/(T) \longrightarrow \mathbb{R}[X]/(X^n - 1)$$

Enfin, comme $(1, 0)$ est un élément idempotent non trivial de A, il en est de même de $\psi(1, 0)$ dans $\mathbb{R}[X]/(X^n - 1)$.

Le lecteur aura remarqué dans le cas n un nombre premier que $Spec(\mathbb{R}[X]/(X^n - 1))$ a exactement deux composantes connexes.

2.1.2 Algèbres séparables

Nous abordons ce paragraphe par un préliminaire d'algébre commutative :

Un anneau S est dit artinien si pour toute chaîne d'idéaux :

$$\mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset ... \supset \mathfrak{a}_n \supset \mathfrak{a}_{n+1} \supset ...$$

il existe un entier positif n tel que $\mathfrak{a}_n = \mathfrak{a}_{n+1}$.

Lemme 19 *Dans un anneau artinien tout idéal premier est maximal.*

Démonstration Soit $\mathfrak{p}$ un idéal premier d'un anneau S artinien. Donc $S/\mathfrak{p}$ ne possède pas d'éléments nilpotents autre que 0 et donc si $x \in S$ est non nul, x^n est non nul pour tout entier $n \geq 0$. Or la suite :

$$xS/\mathfrak{p} \supset x^2S/\mathfrak{p} \supset ... \supset x^nS/\mathfrak{p} \supset x^{n+1}S/\mathfrak{p} \supset ...$$

doit être stationnaire. Donc il existe un entier $k \geq 1$ tel que $x^k = x^{k+1}a$ pour $a \in S/\mathfrak{p}$ et comme $S/\mathfrak{p}$ est intègre, x est inversible.

Lemme 20 *Tout anneau artinien possède un nombre fini d'idéaux premiers*

Démonstration Supposons qu'il existe une suite $(\mathfrak{p}_n)_{n\in\mathbb{N}}$ d'idéaux premiers deux à deux distincts. Alors pour tout entier $m \geq 0$, aucun des $\mathfrak{p}_i$ n'est inclus dans l'un des $\mathfrak{p}_1, ..., \mathfrak{p}_{i-1}, \mathfrak{p}_{i+1}, ..., \mathfrak{p}_{m+1}$ pour $i = 0, 1, 2, ..., m+1$ puisque chaque $\mathfrak{p}_i$ est maximal. Donc il existe $x_j \in \mathfrak{p}_j$ tel que $x_j \notin \mathfrak{p}_{m+1}$ pour tout $j = 0, 1, 2, ..., m$. Donc $x = x_0x_1...x_m$ appartient à tous les $\mathfrak{p}_0, ..., \mathfrak{p}_m$ mais pas à $\mathfrak{p}_{m+1}$. Donc la suite d'ideaux :

$$\mathfrak{p}_0 \supset \mathfrak{p}_0 \cap \mathfrak{p}_1 \supset ... \supset \bigcap_{i=0}^{m} \mathfrak{p}_i \supset \bigcap_{i=0}^{m+1} \mathfrak{p}_i \supset ...$$

est strictement décroissante et ceci contredit le fait que notre anneau est artinien.

Lemme 21 *Toute algébre de dimension finie sur un corps est artinienne en tant qu'anneau.*

Démonstration Soit A une algébre de dimension finie sur un corps K. Supposons que l'on ait une suite d'idéaux strictement croissante :

$$\mathfrak{a}_0 \supset \mathfrak{a}_1 \supset ... \supset \mathfrak{a}_n \supset \mathfrak{a}_{n+1} \supset ...$$

Soit B_0 une base de $\mathfrak{a}_0$ sur K. Donc $\mathfrak{a}_1$ admet une base incluse dans B_0. Ainsi de proche en proche, on a une suite strictement décroissantes d'ensembles :

$$B_0 \supset B_1 \supset ... \supset B_n \supset B_{n+1} \supset ...$$

où pour tout $i \in \mathbb{N}$, B_i est une base de $\mathfrak{a}_i$. Or ceci est contradictoire puisque B_0 est un ensemble fini.

Théorème 12 *Toute algébre non nulle de dimension finie sur un corps est produit fini d'anneaux locaux dont chacun d'entre eux a pour idéal maximal l'idéal engendré par les éléments nilpotents.*

Démonstration Soit A une algébre de dimension finie sur un corps K. Par ce qui précéde, $Spec(A)$ est un ensemble fini de points fermés $\{\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_n\}$. Supposons $n > 1$, le cas $n = 1$ se vérifie aisément. Soit e_i un élément idempotent tel que $V(e_i) = \{\mathfrak{p}_i\}$. Puisque

$$\{\mathfrak{p}_1\} \cap \{\mathfrak{p}_2\} \cap ... \cap \{\mathfrak{p}_n\} = \emptyset$$

il existe $u_1, u_2, ..., u_n$ tel que $\sum_{i=1}^{n} u_i e_i = 1$. Ensuite, $u_i e_i$ est un idempotent et on l'isomorphisme :

$$A \longrightarrow \prod_{i=1}^{n} u_i e_i A = \prod_{i=1}^{n} B_i$$

Donc en examinant les idéaux premiers de A, B_i a un seul idéal premier qui est donc maximal. Enfin, on conclut puisque dans un anneau l'intersection de tous les idéaux premiers est l'idéal des nilpotents.

Définition Un anneau est dit réduit s'il ne posséde pas d'éléments nilopotents.

Corollaire 7 *Toute algébre réduite non nulle de dimension finie sur un corps K est produit fini de corps dont chacun d'entre eux est une extension finie de K.*

Nous rappelons maintenant quelques faits de la théorie des extensions de corps. Pour tout corps D, on note D^a la clôture algébrique de D. Soit E/K une extension algébrique. Si L et L' sont deux corps algébriquement clos contenant K, alors on peut montrer que l'on une bijection entre $Hom_K(E, L)$ et $Hom_K(E, L')$ et que lorsque $[E : K]$ est fini égal à n , $Hom_K(E, L)$ a au plus n éléments. Le cardinal de $Hom_K(E, L)$ est dénoté par $[E, K]_s$.

Définition Si E/K est de dimension égale à n alors elle est dite séparable si $[E, K]_s$ a exactement n éléments.

En fait cette dernière notion est liée à la notion d'éléments séparables :

Définition Soit α un élément de E. α est un élément séparable sur K si son polynôme irreductible sur K n'a pas de racines multiples dans K^a.

Lemme 22 *Soit α un élément de E. Alors $K(\alpha)/K$ est séparable si et seulement si α est séparable.*

Démonstration Soit P le polynôme irreductible unitaire de α sur K. Il suffit donc de se rappeler qu'un morphisme $\psi : K(\alpha) \longrightarrow K^a$ est déteminée de manière bijective par $\psi(\alpha)$. Ainsi puisque les $\psi(\alpha)$ décrivent toutes les racines de P, α est séparable si et seulement si le cardinal de $Hom(K(\alpha), K^a)$ est égal au degré de P. Or le degré de P est celui de $K(\alpha)/K$.

Ensuite si $K \subset F \subset E$ est une tour de corps avec $[E : K]$ fini alors on vérifie que $[E : K]_s = [E : F]_s[F : K]_s$ ce qui nous donne le résultat :

Théorème 13 *Une extension de dimension finie est séparable si et seulement si tous ces éléments sont séparables.*

La définition suivante est inspirée du résultat ci-dessus :

Définition Une extension E/K de dimension finie ou non est dite séparable si tout élément de celle-ci est séparable. Ainsi la composée de deux extensions séparables est séparable et on appelle clôture séparable la composée de toutes les extensions D/E séparable dans E^a/E, on la dénote par E^s.

Pour une extension galoisienne L/K on note $G_{L/K}$ son groupe de Galois. Nous utiliserons aussi les résultats :

Théorème 14 *Le groupe des automorphismes de corps de K^s laissant fixe K est égal à la limite inductive $lim_L G_{L/K}$ où L/K parcourt toutes les extensions galoisiennes finies.*

Proposition 42 *Soient T/K et M/T des extensions de corps et A une algébre sur K alors on a la règle de changement de bases*

$$A \otimes_K M \cong (A \otimes_K T) \otimes_T M$$

Nous pouvons maintenant parler d'algébres séparables :

Proposition 43 *Soit A une algébre de dimension finie sur le corps K. Il y a équivalence entre les propositions suivantes :*
$(AS1)$ L'algébre $A \otimes K^a$ est réduite.
$(AS2)$ $A \otimes K^a$ est isomorphe à un produit $K^a \times ... \times K^a$
$(AS3)$ le cardinal de $Hom_K(A, K^a)$ est égale à la dimension de A sur K.
$(AS4)$ $A \otimes K^s$ est isomorphe à un produit $K^s \times ... \times K^s$

Démonstration Tout d'abord le fait $(AS1)$ implique $(AS2)$ provient des résultats précédents. $(AS2)$ implique $(AS3)$ provient de la bijection :

$$\psi : Hom_K(A, K^a) \ni f \longmapsto \sum_\alpha a_\alpha \otimes \lambda_\alpha \mapsto \sum_\alpha f(a_\alpha) \otimes \lambda_\alpha \in Hom_{K^a}(A \otimes K^a, K^a)$$

Ensuite en utilisant, $dim_{K^a}(A \otimes K^a) = dim_K(A) = n$, il vient $A \otimes K^a \cong (K^a)^n$ et $Hom_{K^a}(A \otimes K^a, K^a)$ a exactement n morphismes. Le point délicat est de

démontrer $(AS3)$ implique $(AS4)$. On observe qu'il suffit de montrer que A est un produit fini d'extensions de corps séparables. Ecrivons $A = A_1 \times ... \times A_m$ avec A_i un anneau local d'idéal maximal $\mathfrak{o}_i$ pour $i = 1, 2, ..., m$. On observe qu'un mophisme de A vers K^a envoie un et seul idempotent de A vers un élément non nul qui est 1. Ce qui montre que l'on a les unions disjointes :

$$Hom_k(A, K^a) = Hom_K(A_1, K^a) \cup Hom_K(A_2, K^a) \cup ... \cup Hom_K(A_m, K^a)$$

Soient $i \in \{1, 2, ..., m\}$ et $\psi : A_i \longrightarrow K^a$ un morphisme. Alors ψ se factorise en un morphisme $overline\psi : L_i \longrightarrow K^a$ avec L_i/K une extension de dimension finie puisque $\mathfrak{o}_i$ est envoyé sur 0. Ensuite les conditions $[L_i : K]_s \leq [L_i : K] \leq dim_K(A_i)$ et $\sum_{i=1}^m [L_i : K]_s = dim_K(A)$ forcent : $[L_i : K]_s = [L_i : K] = dim_K(A_i)$. ce qui donne

$$[L_i : K] = dim_K(A_i) = dim_K(L_i \oplus \mathfrak{o}_i) = [L_i : K] + dim_K(\mathfrak{o}_i)$$

Donc $\mathfrak{o}_i$ est nul et A est produit fini d'extensions séparables finies. Enfin, $(AS4)$ implique $(AS1)$ car :

$$(A \otimes_K K^s) \otimes_{K^s} K^a \cong A \otimes_K K^a$$

Lorsque A vérifie $(AS1), (AS2), (AS3)$ ou $(AS4)$ alors A est dite séparable. En résumé :

Définition alternative Une algébre de dimension finie sur corps K est dite séparable si elle est produit d'extensions séparables finies de K.

Nous allons voir les algébres séparables sous un nouveau angle. Soit X un ensemble fini et K un corps et notons G le groupes des automorphismes de corps de K^s laissant fixe K.

Définition Soit $\pi : G \longrightarrow \mathfrak{S}_X$ une action de groupe G sur X. On dit que π est continue si X est l'union d'ensembles $X_1, X_2, ..., X_m$ stables par l'action de G tels que pour tout $i = 1, 2, ...m$, le morphisme $\pi_i : G \longrightarrow \mathfrak{S}_{X_i}$ se factorise en un morphisme $\overline{\pi}_i : G_{L_i/K} \longrightarrow \mathfrak{S}_{X_i}$ avec L_i/K une extension galoisiennne finie.

Pour alléger le discours, lorsque G opère continûment sur X, nous dirons que X est un G-ensemble et nous noterons $g.x = \pi(g)(x)$ pour tout $x \in X$ et $g \in G$.

Définition Soient X, Y deux G-ensembles finis. Une application $f : X \longrightarrow Y$ est un morphisme de G-ensembles si pour tout $g \in G$ et pour tout $x \in X$, $f(g.x) = g.f(x)$.

Lemme 23 *Tout G-ensemble fini est isomorphe au G-ensemble $Hom_K(A, K^s)$ muni de l'action $(\sigma.f)(a) = \sigma \circ f(a)$ pour tout $a \in A$ et $\sigma \in G$ avec A une certaine algébre séparable sur K.*

Démonstration Pour X un G-ensemble fini, montrons qu'il existe une algèbre séparable A sur K telle que $Hom_K(A, K^s)$ soit un G-ensemble isomorphe à X. Si O est une orbite d'un point $x \in X$ alors l'action de G se factorise en une action de $G_{K/L}$ avec K/L une extension galoisienne finie. Ainsi, on se limite pour l'instant au cas $X = O$. Soient $S \subset G_{L/K}$ le sous-groupe d'isotropie de x, D le sous-corps invariant sous l'action de S et $g_1, g_2..., g_N$ des représentants de classes de $G_{L/K}$ modulo S. On a donc l'isomorphisme :

$$\psi : G_{L/K}/S \ni g_j.x \longmapsto g_j \circ i \in Hom_K(D, L)$$

En effet, ψ est bien définie puisque L/K est galoisienne, l'injectivité est déduite directement et la surjectivité provient du fait que tout morphisme de D vers L se prolonge en un automorphisme de L. Or $Hom_K(D, L)$ s'indentifie à $Hom_K(D, K^s)$, on a donc résolu le cas $X = O$. Maintenant pour le cas général, on considère toutes les orbites de $O_1, O_2, ..., O_m$ et $D_1, D_2, ..., D_m$ les sous-corps de K^s invariant par les sous-groupes s'isotopies sous-jacent, ainsi les unions disjointes :

$$Hom_K(D_1, K^s) \cup Hom_K(D_2, K^s) \cup ... \cup Hom_K(D_n, K^s) = Hom_K(A, K^s)$$

nous déterminent l'isomorphisme de $G-$ensembles entre X et $Hom_K(A, K^s)$.

Soit X un G-ensemble fini. On considére l'algébres $F(X)$ l'algébres des fonctions de X vers K^s. On munit $F(X)$ d'une structure de G-ensembles en posant :

$$(\sigma.f)(x) = \sigma \circ f(\sigma^{-1}.x)$$

pour tout $\sigma \in G$, pour tout $f \in F(X)$ et pour tout $x \in X$. Le lemme nous permet de déterminer A à partir de X :

Lemme 24 *Pour tout G-ensemble fini X les éléments de $F(X)$ invariants sous l'action de G forment une algébre séparable.*

Démonstration Par le lemme précédent, on peut donc poser $X = Hom(A, K^s)$. Soit $\phi : A \otimes K^s \longrightarrow F(X)$ l'isomorphisme d'algébres qui à $a \otimes \lambda$ associe la fonction f telle que $f(x) = x(a)\lambda$. Ainsi l'action définie par $\sigma(a \otimes \lambda) = a \otimes \sigma(\lambda)$ pour tout $\sigma \in G$ se traduit via ϕ par :

$$x(a)\sigma(\lambda) = \sigma.(\sigma^{-1}.x(a)\lambda) = (\sigma.f)(x)$$

ce qui donne un isomorphisme de G-ensembles. Enfin, on conclut en remarquant que l'algébre fixée par G de $A \otimes K^s$ est A.

Théorème 15 *Les G-ensembles finis sont anti-équivalents aux algébres séparables de dimension finie sur K.*

Démonstration Soient A, B des algèbres séparables sur le corps K. Il s'agit de montrer que $Hom_K(A,B)$ est eb bijection avec $Hom_G(X_B, X_A)$ où X_A désigne $Hom_K(A, K^s)$ muni de l'action : $(g.f)(x) = g \circ f(x)$ pour tout $g \in G$, pour tout $f \in X_A$ et pour tout $x \in A$. Soit $\psi : A \longrightarrow B$ un morphisme entre deux algébres séparables finies. Alors ψ induit un morphisme $X(\psi) : X_B \longrightarrow X_A$ en composant $f \in X_B$ par ψ. Inversement, si $T : X_B \longrightarrow X_A$ est un morphisme alors cela donne un morphisme $F(T) : F(X_A) \longrightarrow F(X_B)$ et il s'ensuit que les éléments invariants de $F(X_A)$ sont envoyés vers les éléments invariant de $F(X_B)$ et par lemme précédent on a un morphisme de A vers B.

2.1.3 Schéma en groupe étale

Définition Un schéma en groupe affine fini sur un corps est étale s'il est représenté par une algébre séparable.

On note comme ci-dessus G le groupe des automorphismes de K^s laissant fixe K.

Théorème 16 *Les schémas en groupes affines étales et finis sont équivalents aux groupes finis munis d'une structure de G-ensembles.*

Démonstration Soit A une algébre de Hopf séparable de dimension finie sur un corps K. Alors la comultiplication $M : A \longrightarrow A \otimes A$, le morphisme coinverse $S : A \longrightarrow A$ et l'augmentation $\varepsilon : A \longrightarrow K$ munisse X_A de morphismes $X(M) : X_A \times X_A \longrightarrow X_A$, $X(S) : X_A \longrightarrow X_A$ et $\{id\} \longrightarrow X_A$ qui confèrent à X_A une structure de groupe.

Proposition 44 *Pour tout entier $n \geq 1$, le schéma en groupe μ_n sur le corps $\mathbb{Q}$ est étale.*

Démonstration Montrons que $\mathbb{Q}[X]/(X^n - 1)$ est une algébre séparable pour X une indéterminée. Pour cela, on a la formule :

$$X^n - 1 = \prod_{p|n} \Phi_p(X)$$

où le produit parcourt tous les nombres premiers p divisant n. ($\Phi_p(X)$ est le p-ième polynômes cyclotomique.) Or puisque tous les $\Phi_p(X)$ sont irreductibles sur $\mathbb{Q}$ et deux à deux distincts, par le théorème Chinois :

$$\mathbb{Q}[X]/(X^n - 1) \cong \prod_{p|n} \mathbb{Q}[X]/\Phi_p(X) \cong \prod_{p|n} \mathbb{Q}(\zeta_p)$$

avec ζ_p une racine p-ième de l'unité. Ensuite, on sait que $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ est une extension galoisienne.

Le résultat suivant nous permettra de simplifier de nombreux raisonnements :

Proposition 45 *Si L/K une extension de corps alors une algébre A sur K est séparable si et seulement si $A \otimes L$ est séparable sur L.*

Démonstration Si A est une algébre séparable sur K alors :

$$(A \otimes L) \otimes_L L^a \cong (A \otimes K^a) \otimes_{K^a} L^a \cong L^a \times L^a \times ... \times L^a$$

Donc $A \otimes L$ est séparable par la condition $(AS2)$. Si $A \otimes L$ est séparable alors par $(AS1)$, $A \otimes L^a$ est réduite et il en est de même de $A \otimes K^a$. Donc A est séparable.

Corollaire 8 *Pour tout entier n, μ_n sur tout corps de caractéristique nulle est étale.*

Soit E un schéma en groupe affine représenté par une algébre de Hopf A de type finie sur un corps K.

Proposition 46 *Il existe une unique algébre dimension finie sur K qui soit séparable, contenue dans A et maximale pour l'inclusion.*

Par les caractérisations précédentes, le quotient et produit tensoriel d'algébre séparables est séparable. Pour abréger toute nos algébres séparables seront de dimensions finies :

Démonstration Soit B une sous-algébre séparable. Donc $B \otimes K^a$ est une sous-algébre séparable de $A \otimes K^a$ et par $(AS2)$, $B \otimes K^a$ est engendré par les idempotents N. Donc $dim_K(B) = dim_{K^a}(B \otimes K^a)$ est majorée par le nombre de nilpotents de A qui est fini puisque A est noethérien. Donc toute chaîne d'algébres séparables

$$B_0 \subset B_1 \subset B_2 \subset ... \subset B_n \subset B_{n+1} \subset B_{n+2}...$$

est stationnaire à partir d'un certain rang. Soit maintenant X l'ensemble de toutes les sous-algébres séparables. Alors X possède un élément maximal. En effet, dans le cas contraire nous pouvons construire une chaîne d'algébres séparables non stationnaire. Il reste donc à montrer l'unicité. Si B, C sont deux éléments maximaux de X alors la composée BC est un quotient $B \otimes C$ donc est séparable. Si $B \neq C$ alors $B \subset BC$ est stricte, ce qui est une contradiction.

Pour toute algébre R de type fini sur K, on note $\pi_0(R)$ la sous-algébre séparable maximale. Nous allons montrer ci-après qu'en fait $\pi_0(R)$ est une sous-algébre de Hopf.

Lemme 25 *Soit R une algébre de type fini sur un corps K. Si R s'ecrit $R_1 \times R_2 \times ... \times R_n$ avec R_i des algébres alors $\pi_0(R) = \pi_0(R_1) \times \pi_0(R_2) \times ... \times \pi_0(R_n)$.*

Démonstration Montrons le resultat pour deux facteurs S et T, le cas général s'effectuant par récurrence. Tout d'abord, on par définition de π_0, $\pi_0(S) \times \pi_0(T) \subset \pi_0(S \times T)$.

Lemme 26 *Soit α un élément algébrique de polynôme minimal P sur K.*
(a) Si K est de caractéristique nulle alors P est à racine simple.
(b) Si K est de caractéristique un nombre premier $p > 0$ alors il existe un entier $\mu \geq 0$ tel que α^{p^μ} soit séparable.

Démonstration Soient $\alpha, \alpha_2, ..., \alpha_n$ les racines distinctes de P. Donc P s'ecrit

$$(X-\alpha)^m(X-\alpha_2)^{m_2}(X-\alpha_2)^{m_2}...(X-\alpha_n)^{m_n}$$

Ensuite, le morphisme $\sigma : K(\alpha) \longrightarrow K^a$ envoyant α sur α_2 se prolonge en un automorphisme sur K^a et P s'ecrit également :

$$(X-\alpha)^{m_2}(X-\alpha_2)^{m}(X-\alpha_3)^{m_3}...(X-\alpha_n)^{m_n}$$

En appliquant le même raisonnement pour chaque facteur, il vient $m = m_i$ pour $i = 2, 3, ..., n$. Si K est de caractéristique nulle alors et $m > 1$ alors P' est nul et $P'(\alpha) = 0$, ce qui est contradictoire. Donc $m = 1$. Maintenant si K est de caractéristique $p > 0$ et $P' = 0$ alors il existe un entier $\nu > 0$ tel que $m = p^\nu$ et

$$P = (X-\alpha^m)(X-\alpha_2)^m...(X-\alpha_n)^m = (X^m-\alpha^m)...(X^m-\alpha_n^m) = Q(X^m)$$

Supposons qu'il existe $R \in K[X]$ tel que R divise Q. Donc $R(X^m)$ divise $Q(X^m) = P$ et cela force R inversible. Donc Q est irreductible et enfin si Q est de degré d alors :

$$[K(\alpha^{p^\nu}) : K] = d = [K(\alpha^{p^\nu}) : K]_s$$

Théorème 17 *Si L/K est une extension de corps alors :*

$$\pi_0(A) \otimes L = \pi_0(A \otimes L)$$

Démonstration En premier lieu, $\pi_0(A) \otimes L \subset \pi_0(A \otimes L)$ et écrivons $A = A_1 \times A_2 \times ... \times A_n$ avec n le nombre de composante connexe de $Spec(A)$. Puiqu'il reste à vérifier l'égalité des dimensions, le résultat ci-dessus est vrai si l'on suppose K et L séparablement clos. Par suite $\pi_0(A_i) = K$ et $\pi_0(A)$ est engendré par des idempotents, disons $e_1, e_2, ..., e_n \in K^s$ (car $\pi_0(A) \cong F(X)$ pour un certain ensemble fini.). Si K n'est pas algébriquement clos alors $\pi_0(A \otimes K^a)$ est également engendré par des idempotents $f_1, ..., f_n$ et par un lemme précédent, il existe un nombre premier p et un entier $\nu \geq 0$ tels que $f_i^{p^\nu}$ appartienne à $\pi_0(A)$. Donc sans perte de généralité, on pose $e_i = f_i^{p^\nu}$ et on suppose K et L algébriquement clos. Enfin, puisque $\pi_0(A \otimes L) = \pi_0(A_i \otimes L) \times ... \times \pi_0(A_n \otimes L)$, il reste à montrer que $\pi_0(A_i \otimes L)$ ne posséde pas d'idempotents non triviaux et ceci est dû au fait suivant :

Proposition 47 *Tout ensemble algébrique irreductible sur un corps algébriquement clos est connexe. Soient K/L une extension de corps avec K et L algébriquement clos et $\mathfrak{a}$ un idéal de $K[X_1, ..., X_n]$. Si $Z_K(\mathfrak{a})$ est irreductible alors $Z_L(\mathfrak{a})$ est irreductible.*

Démonstration Le premier point vient du fait qu'un anneau intégre ne possède pas d'idempotents non triviaux. Notons $X = (X_1, ..., X_n)$. Supposons que $Z_L(\mathfrak{a})$ ait pour composantes irreducitbles $S_1, S_2, ..., S_m$. Alors pour tout i, $S_i \cap K^n$ est irreductible et :

$$Z_K(\mathfrak{a} = S_1 \cap K^n \cup S_2 \cap K^n \cup ... \cup S_m \cap K^n$$

Ce qui est une contradiction.

Lemme 27 *Soit S et T deux ensembles algébriques connexes sur un corps algébriquement clos alors $S \times T$ est un ensemble algébrique connexe.*

Démonstration Soient K un corps algébriquement clos, $X = (X_1, X_2, ..., X_n)$, $Y = (Y_1, ..., Y_n)$ des systèmes d'indéterminées, $P_1(X) = P_2(X) = ... = P_l(X) = 0$ les équations de S et $Q_1(Y) = Q_2(Y) = ... = Q_k(Y) = 0$ les équations de T. Donc $S \times T$ est un ensemble algébrique de K^{2n} et a pour équation :

$$P_1(X) = P_2(X) = ... = P_l(X) = Q_1(Y) = Q_2(Y) = ... = Q_k(Y) = 0$$

Ensuite, montrons que pour tous points $p, q \in S \times T$, il existe une partie connexe C telle que $p, q \in C$. Notons $p = (s_1, t_1)$, $q = (s_2, t_2)$ et

$$C = \{s_1\} \times T \cup S \times \{t_1\} \cup \{s_2\} \times T \cup S \times \{t_2\}$$

que nous dénotons dans le même ordre par :

$$C = R_1 \cup R_2 \cup R_2 \cup R_4$$

On a $R_i \cap R_{i+1} \neq \emptyset$ pour $i = 1, 2, 3$ et chaque R_i est connexe, d'où le résultat.

Théorème 18 *Soient R, S deux algébres de type fini sur le corps K. Alors $\pi_0(R \otimes S) = \pi_0(R) \otimes \pi_0(S)$.*

Démonstration Supposons K algébriquement clos comme précédemment. On a : $\pi_0(R) \otimes \pi_0(S)$ par définition de π_0. Après décomposons $R = R_1 \times ... \times R_n$ et $S = S_1 \times ... \times S_m$ avec m, n le nombre de composantes connexes de R et S. Donc pour tous i, j, $\pi_0(R_i) \otimes \pi_0(S_j) \cong K$ et il reste à montrer que $\pi(A_i \times A_j)$ ne possède pas d'idempotents. Or cela est vrai par le lemme précédent.

Proposition 48 *$\pi_0(A)$ est une sous-algébre de Hopf de A.*

Démonstration Soient $B \subset A$ une sous-algébre séparable et M la comultiplication de A. Alors $M(B)$ est isomorphe au quotient de B par le noyau de la restriction de M à B. Donc $M(B)$ est separable. Donc pour $B = \pi_0(A)$

$$(M|\pi_0(A))(\pi_0(A)) \subset \pi_0(A \otimes A) = \pi_0(A) \otimes \pi_0(A)$$

Définition On note $\pi_0(E)$ le schéma en groupe affine représenté par $\pi_0(A)$.

Proposition 49 *$\pi_0(E)$ est réduit à élément neutre si et seulement si le schéma affine $Spec(A)$ est connexe.*

Démonstration Si $Spec(A)$ est connexe alors $\pi_0(A)$ est un corps L contenant K (car $\pi_0(A)$ est produit d'extension séparable et n'a pas d'idempotents.) Donc l'augmentation $\varepsilon : L \longrightarrow K$ est un morphisme de corps, ce qui contraint $K = L$. La réciproque se vérifie aisèment.

Définition L'inclusion de $\pi_0(A)$ vers A induit un morphisme surjectif de E vers $\pi_0(E)$. On note E^0 le noyau de ce morphisme, on l'appelle la composante connexe de E.

Par le chapitre précédent, nous savons que le noyau du morphisme naturel $A \longrightarrow \pi_0(A)$ est une immersion fermée de A et est représenté par $A/(I \cap \pi_0 A).A$ où I est le noyau de l'augmantation ε. Il s'ensuit :

Corollaire 9 *E^0 est connexe.*

Démonstration Ecrivons $A = A_1 \times ... \times A_n$ avec n le nombre composantes connexes et

$$e_i = (0, 0, ..., 0, 1, 0, ..., 0)$$

la liste à n éléments avec 1 en i-ème position. Donc $\pi_0(A) = e_1\pi_0(A) \oplus ... \oplus e_n\pi_0(A)$ qui est en fait la décomposition de $\pi_0(A)$ en produit d'extensions séparables. Soit alors i l'unique entier tel que $\varepsilon(e_i) = 1$. Donc $(1 - e_i)\pi_0(A) = I \cap \pi_0(A)$. Donc par la proposition précédente E^0 est représenté par $A^0 = A/((1 - e_i)\pi_0 A)A \cong e_i A$. Ainsi, par factorisation de ε, $A^0 \cong K$ et donc E^0 est connexe.

Proposition 50 *Soient F un schéma en groupe affine étale, $\Phi : E \longrightarrow F$ un morphisme et $\pi : E \longrightarrow \pi_0 E$ le morphisme naturel. Alors il existe un unique morphisme $\overline{\Phi} : \pi_0 E \longrightarrow F$ tel que $\Phi = \overline{\Phi} \circ \pi$.*

Démonstration L'unicité est automatique puisque π est surjectif. Montrons l'existence. Notons B l'algèbre de Hopf représentant F et $u : B \longrightarrow A$ le morphisme déduit de Φ. On observe que l'image de B par u est séparable car est quotient de B. Donc u induit un morphisme $\overline{u} : B \longrightarrow \pi_0 A$ qui à $x \in B$ associe $u(x)$. Ainsi on a la suite :

$$B \xrightarrow{u} \pi_0 A \xrightarrow{i} A$$

avec $i : \pi_0 A \longrightarrow A$ l'inclusion. Ce qui donne les morphismes :

$$E \xrightarrow{\pi} \pi_0 E \xrightarrow{\overline{\Phi}} F$$

Nous pouvons être plus précis lorsque le corps de base est parfait, pour cela :

Définition Un corps est dit parfait si toute extension algébrique de celui-ci est séparable.

En utilisant la dérivée de polynômes, on en déduit que $\mathbb{Q}$ est un corps parfait et donc tout corps de caractéristique nulle est parfait.

Proposition 51 *Une algébre de dimension finie sur un corps parfait est séparable si et seulement si elle est réduite.*

Démonstration En fait seule la réciproque est à vérifier. Si R est une algébre réduite de dimension finie sur K un corps alors R est produit de corps $L_1 \times ... \times L_n$. Or L_i/K sont des extensions algébriques car finies et donc si K est parfait, L_i/K est séparable.

Nous désignons par N l'idéal des éléments nilpotents de A. On rappelle que N est l'intersection de tous les idéaux premiers de A

Lemme 28 *Si K est parfait alors $\pi_0(A)$ est isomorphe à A/N.*

Démonstration Montrons que $\pi_0(A)$ est isomorphe à $\pi_0(A/N)$. Puisque $\pi_0(A)$ ne posséde pas de nilpotents il est donc contenu dans le supplémentaire de N qui est isomorphe à A/N. Donc on a un morphisme injectif $\pi_0(A) \longrightarrow \pi_0(A/N)$. Ainsi, il suffit de montrer l'égalité des dimensions et on suppose K algébriquement clos. Enfin, la dimension de $\pi_0(A)$ correspond au nombre de composantes connexes de A et puisque $Spec(A)$ et $Spec(A/N)$, on a $\pi_0(A) \cong \pi_0(A/N) \cong A/N$.

Nous clôturons ce paragraphe par le résultat suivant :

Théorème 19 *Tout schéma en groupe affine E fini sur un corps parfait est produit semi-direct de $\pi_0(E)$ et de sa composante connexe E^0.*

Démonstration Montrons que $\pi_0(A)$ représente une immersion fermée de E. Si M est la comultiplication de A alors on a la suite de morphismes :

$$A \xrightarrow{M} A \otimes A \xrightarrow{p} A/N \otimes A/N$$

se factorisant en un morphisme $A/N \longrightarrow A/N \otimes A/N$, d'où la première affirmation. Notons $\pi : A \longrightarrow A/N$ le morphisme de passage aux quotients et $i : \pi_0(A) \longrightarrow A$ l'inclusion. On a donc la suite de morphismes pour toute algébre R sur K :

$$Hom(A/N, R) \xrightarrow{\Phi_1} Hom(A, R) \xrightarrow{\Phi_2} Hom(\pi_0 A, R)$$

où $\Phi_1(\psi) = \psi \circ \pi$ et $\Phi_2(\alpha) = \alpha \circ i$ pour tout $\psi \in Hom(A/N, R)$ et $\alpha \in Hom(A, R)$. Donc si $\psi \in Hom(A/N, R)$ alors $\Phi_1 \circ \Phi_2(\psi) = \psi \circ \pi \circ i$. Or $\pi \circ i$ est un isomorphisme de $\pi_0(A)$ vers A/N et donc $\Phi_1 \circ \Phi_2$ est isomorphisme à l'identité. On conclut par un résultat du chapitre précédent.

2.2 Schéma en groupe affine lisse

2.2.1 Formes différentielles

Soit A une algébre sur un anneau B et V un module sur A. En particulier, V est un module sur B.

Définition Un morphisme $D : A \longrightarrow V$ de module sur B est une dérivation si pour tous $x, y \in A$ on a :

$$D(xy) = xD(y) + D(x)y$$

En particulier, on a pour tout $a \in B$:

$$D(a) = D(a1_A) = aD(1_A) = a(1_A D(1_A) + D(1_A)1_A) = 2D(a)$$

et $D(a) = 0$. On note $\mathfrak{D}_A$ la catégorie des dérivations $D : A \longrightarrow V$ avec V un module sur A et dont un morphisme de D vers $D' : A \longrightarrow W$ est un morphisme $\psi : V \longrightarrow W$ de modules sur A tel que : $D' = \psi \circ D$. Nous allons montrer que $\mathfrak{D}_A$ posséde un objet universel :

Soit $\Omega_{A/B} = \Omega(B/A)$ le module sur A engendré par les symboles formelles dx avec x un élément de A sous les seuls contraintes :

$$d(x + y) = dx + dy$$

$$d(xy) = xdy + ydx$$

et $da = 0$ pour tous $x, y \in A$ et $a \in B$. $\Omega_{A/B}$ est un module sur B et l'application $d : A \longrightarrow \Omega_{A/B}$ qui à tout $x \in A$ associe dx est une dérivation. $\Omega_{A/B}$ est appelé le module des formes différentielles et lorsque la mention de B est claire on le dénote par $\Omega_A = \Omega(A)$.

Théorème 20 *Pour toute dérivation D de A vers un module V sur A, il existe un unique morphisme de $d : A \longrightarrow \Omega_A$ vers D.*

Démonstration Soient D une dérivation de A vers V et $\psi : \Omega_A \longrightarrow V$ le morphisme qui à dx associe $\psi(dx) = D(x)$, ψ est bien définie et est unique par définition de Ω_A. Donc $d : A \longrightarrow \Omega$ est un objet initial dans $\mathfrak{D}_A$, il est donc unique à isomorphisme près.

Corollaire 10 *Soit V un module sur A. Si l'on note $D(A, V)$ le module des dérivations de A vers V alors on a un isomorphisme naturel :*

$$D(A, V) \longrightarrow Hom(\Omega_A, V)$$

Démonstration On considère l'application Φ qui à tout morphisme $\psi \in Hom(\Omega_A, V)$ associe $\psi \circ d$. Par universalité de d, Φ est injectif. De plus, Φ est surjectif car pour une dérivation D, on prend $\psi \in Hom(\Omega_A, V)$ tel que $\psi(dx) = D(x)$ pour tout $x \in A$.

Examinons le cas où B est un corps K et A une algébre de type fini sur K. Soit $X = (X_1, X_2, ..., X_n)$ un système d'indéterminées.

Proposition 52 *Si $\mathfrak{a} = (P_1, ..., P_m)$ est un idéal de $K[X]$ et $A = K[X]/\mathfrak{a}$ alors Ω_A est le module libre sur A de vecteurs de base $dx_1, dx_2, ..., dx_n$ modulo le sous-module engendré par les vecteurs :*

$$\frac{\partial P_i}{\partial X_1}dx_1 + \frac{\partial P_i}{\partial X_2}dx_2 + ... + \frac{\partial P_i}{\partial X_n}dx_n$$

pour tout entier $i = 1, 2, ..., m$.

Démonstration Il suffit de montrer que le Ω_A proposé satifait la propriété universelle. On observe que $\Omega_{K[X]}$ est le module libre sur $K[X]$ engendré par $dx_1, dx_2, ..., dx_n$. Notons Ω le module quotient de $\Omega_{K[X]}$ par le sous-module $I = \mathfrak{a}\Omega_{K[X]} + K[X]d\mathfrak{a}$ et soit $D : A \longrightarrow V$ une dérivation avec V un module sur A. Alors la composition :

$$K[X] \xrightarrow{\pi} A \xrightarrow{D} V$$

est une dérivation T de $K[X]$ vers V. Donc il existe un unique morphisme $\psi : \Omega_{K[X]} \longrightarrow V$ tel que $T = \psi \circ d$. Donc par fonctorialité du passage aux quotients :

$$D = \overline{\pi \circ D} = \overline{T} = \overline{\psi \circ d} = \overline{\psi} \circ \overline{d}$$

$\overline{\psi}$ est donc déterminée de manière unique et $\overline{d} : A \longrightarrow \Omega$ est la dérivation qui à $X_i \bmod \mathfrak{a}$ associe $dX_i \bmod I$. D'où $\Omega \cong \Omega_A$.

Donnons quelques propriétes :

Proposition 53 *Soient R et S deux algèbres de type fini sur un corps K. Alors on a les règles :*
(a) Si L/K est une extension de corps alors $\Omega(R \otimes_K L/L) \cong \Omega_R \otimes_K L$.
(b) $\Omega(R \times S) \cong \Omega_R \times \Omega_S$
(c) Si U est une partie multiplicative de R alors $\Omega(U^{-1}R) \cong \Omega_R \otimes_R U^{-1}R$.

Démonstration Le point (a) se déduit de la proposition précédente. Montrons (b). Soit V un module sur le produit $R \times S$. Notons V_R et V_S les modules V sur $R \times \{0\}$ et $\{0\} \times S$. Donc on a l'isomorphisme

$$V \ni \sum_\alpha (a_\alpha, b_\alpha)v_\alpha \mapsto (\sum_\alpha (a_\alpha, 0)v_\alpha, \sum_\alpha (0, b_\alpha)v_\alpha) \in V_R \times V_S$$

Soient alors $D : R \times S \longrightarrow V$ une dérivation et $D_1 : R \longrightarrow V_R$, $D_2 : S \longrightarrow V_S$ les dérivations déduites de D en restreignant à $R \times \{0\}$ et $\{0\} \times S$. Donc $D = (D_1, D_2)$ et il existe des morphismes uniquement déterminés $\psi_1 : \Omega_R \longrightarrow V_R$, $\psi_2 : \Omega_S \longrightarrow V_S$ tel que $D = (\psi_1, \psi_2) \circ (d_1, d_2)$ avec d_1, d_2 les dérivations universelles de R et S. D'où (b). Montrons (c). On remarque tout d'abord l'isomorphisme :

$$Hom_R(\Omega_R, V) \ni \psi \mapsto \sum_\alpha \frac{a_\alpha}{s_\alpha} \otimes v_\alpha \mapsto \sum_\alpha \frac{a_\alpha}{s_\alpha} \otimes \psi(v_\alpha) \in Hom_R(U^{-1}R \otimes \Omega_R, V)$$

dont l'inverse se calcule aisément.

2.2.2 Théorème de Cartier

Soit B/A une extension d'anneaux, on rappelle qu'un élément $\alpha \in B$ est dit entier sur A s'il existe des éléments $a_0, a_1, ..., a_n$ de A tels que :

$$\alpha^{n+1} + a_n\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0$$

ce qui est équivalent à dire que $A[\alpha]$ est un module de type fini sur A. La relation ci-dessus est dite de dépendance intégrale. B/A est dite entière si tout élément de B est entier sur A.

Le résultat suivant est appelé lemme de normalisation d'Emmy Noether.

Théorème 21 *Toute algébre R de type finie sur un corps K admet un sous-anneau S isomorphe à un anneau de polynômes a plusieurs variables tel R soit un module de type fini sur S. En particulier, R/S est une extension d'anneaux entière.*

Démonstration Soit $\mathfrak{a}$ un idéal de $K[X] = K[X_1, ..., X_n]$ tel que $A \cong K[X]/\mathfrak{a}$. Appelons liste une liste de polynômes $Y = (Y_1, Y_2, ..., Y_n)$ de $K[X]$ tel que $K[X]$ soit un module de type fini sur $K[Y]$. On définit une relation d'ordre partiel sur l'ensemble des listes en posant $Y \leq W$ si W posséde plus de coordonnées appartenant $\mathfrak{a}$. Soit alors $S = (S_1, S_2, ..., S_n)$ une liste maximale et quitte à renuméroter, notons $s_1, s_2, ..., s_r, (1 \leq r \leq n)$ les images non nuls dans A des $S_1, S_2, ..., S_n$. Donc A est un module de type fini sur $K[s] = K[s_1, s_2, ..., s_r]$ et il reste à montrer que $s_1, s_2, ..., s_r$ sont algébriquement indépendants sur K. Supposons le contraire, il existe un polynôme de $f \in K[X_1, ..., X_r]$ tel que $\omega_1 = f(S_1, S_2, ..., S_r)$ soit dans $\mathfrak{a}$. Pour tout entier $i = 2, 3, ..., r$, $\omega_i = S_i - S_1^{m_i}$ avec m_i des entiers $>$ au degré total de f. Donc l'égalité $f(S_1, S_2, ..., S_r) - \omega_1 = 0$ donne une relation de dépendance intégrale

$$Y^N + a_{N-1}(\omega)Y^{N-1} + ... + a_1(\omega)Y + a_0(\omega) = 0$$

avec $a_0, ..., a_{N-1}$ des polynômes de $K[\omega] = K[\omega_1, \omega_2, ..., \omega_r]$ et comme $K[S_1, \omega] = K[S_1, ..., S_r]$, $K[S_1, ..., S_r]$ est un module de type fini sur $K[\omega_2, ..., \omega_r]$. Notons

alors $T = K[\omega_1, ..., \omega_r, S_{r+1}, ..., S_r]$ et soient $f_1, f_2, ..., f_m \in K[X]$ tels que les classes $\overline{f}_1, ..., \overline{f}_m$ engendrent A sous $K[s]$. Donc $K[X]$ est de type fini sur T car enendré par la famille $(f_i S_1^j, j < N)$. Or la liste $(\omega_1, \omega_2, ..., \omega_r, S_{r+1}, ..., S_n)$ est strictement plus grande que S, ce qui est une contradiction.

Dans la démonstration ci-dessus, le lecteur aura remarquer qu'une liste existe puisqu'il suffit de prendre $(X_1^2, X_2^2, ..., X_n^2)$ et vérifiera les cas $r = 0$ et $r = n$. Nous avons également besoin du théorème dit d'intersection de Krull.

Théorème 22 *Soit A un anneau noethérien local d'idéal maximal $\mathfrak{m}$ alors*

$$\bigcap_{n=0}^{\infty} \mathfrak{m}^{n+1} = \{0\}$$

Démonstration Notons $\mathfrak{m} = (a_1, a_2, ..., a_n)$, $A[X] = A[X_1, X_2, ..., X_n]$ et $\mathfrak{a}$ l'idéal des polynômes homogènes P tels que $P(a_1, a_2, ..., a_n) \in \cap_n \mathfrak{m}^n$. Comme $A[X]$ est noethérien, on peut écrire $\mathfrak{a} = (P_1, P_2, ..., P_m)$ et d le maximum des degrés de ces générateurs. Soit $\xi \in \cap_n \mathfrak{m}^n$. Donc $\xi \in \mathfrak{m}^{d+1}$ et donc il existe un polynôme homogéne $P \in A[X]$ de degrés $d+1$ tel que $P(a_1, a_2, ..., a_n) = \xi$. Ensuite $P \in \mathfrak{a}$. Donc il existe des polynômes $s_1, s_2, ..., s_m$ tels que

$$P = s_1 P_1 + s_2 P_2 + ... + s_m P_m$$

Or P est homogène donc ceci force $s_1, ..., s_m$ homogènes de degrés > 0. Donc $\xi \in \mathfrak{m} \cap \cap_n \mathfrak{m}^n$. Ce qui donne $\mathfrak{m} \cap \cap_n \mathfrak{m}^n = \cap_n \mathfrak{m}^n$ et on conclut par le lemme de Nakayama.

Soit A une algébre de type fini sur un corps K.

Lemme 29 *Soit $u : A \longrightarrow K$ un morphisme de noyau $\mathfrak{a}$. On note W un espace vectoriel sur K qui est module sur A par le biais du morphisme u. Alors : $D_K(A, W) \cong Hom_K(\mathfrak{a}/\mathfrak{a}^2, W)$ avec $D_K(A, W)$ les dérivations de A vers W.*

Démonstration A toute dérivation D comme ci-dessus on associe sa focatorisée de $\overline{D}$. En effet, si $xy \in \mathfrak{a}^2$ alors :

$$D(x.y) = u(x)D(y) + u(y)D(x) = 0$$

Inversement, $\psi : \mathfrak{a}/\mathfrak{a}^2 \longrightarrow W$ est un morphisme et $\pi : A \longrightarrow \mathfrak{a}/\mathfrak{a}^2$ est le morphisme qui à $\xi + a \in \mathfrak{a} \oplus K$ associe ξ mod $\mathfrak{a}^2$ alors $\pi \circ \psi$ est une dérivation et $\overline{\pi \circ \psi} = \psi$, ce qui donne le résultat.

Corollaire 11 *Toute algébre de dimension finie sur un corps est séparable si et seulement si son module des formes différentielles est nulle.*

Démonstration Si A est séparable alors quitte à tensoriser, on peut supposer que K est algébriquement clos. Donc $A \cong K \times ... \times K$ et il s'ensuit : $\Omega_A \cong \Omega_K \times ... \times \Omega_K = \{0\}$ puisque $\Omega_K = \{0\}$. Réciproquement, A est de dimension finie donc s'ecrit comme produit $A_1 \times A_2 \times ... \times A_n$ avec A_i des anneaux locaux. Maintenant comme $\Omega_A = \{0\}$ alors focément $\Omega_{A_i} = \{0\}$. Notons $\mathfrak{a}_i$ l'idéal maximal de A_i et $\pi : A_i \longrightarrow k_i = A_i/\mathfrak{a}_i$ la surjection canonique. k_i est donc muni d'une structure de module sur A_i par le morphisme π. Donc par le lemme précédent, $Hom(\Omega_{A_i}, k_i) \cong Hom(\mathfrak{a}_i/\mathfrak{a}_i^2, k_i)$, ce qui force $\mathfrak{a}_i/\mathfrak{a}_i^2 = \{0\}$ soit $\mathfrak{a}_i = \mathfrak{a}_i^2$. Ensuite A_i est noethérien et donc $\mathfrak{a}_i$ est un module de type fini sur A_i. Donc par le lemme de Nakayama $\mathfrak{a}_i = \{0\}$. Donc A est séparable.

Si V est un module sur A alors on note $B = A \oplus V$ l'algébre munie du produit

$$(a, v)(b, w) = (ab, aw + bv)$$

pour tous couples $(a, v), (b, w) \in A \oplus V$.

Lemme 30 *Pour toute algébre R sur K les morphismes de R vers B correspondent aux couples de (ψ, D) où $\psi : R \longrightarrow A$ est un morphisme d'algébres (donc V est un module sur R selon ψ) et $D : R \longrightarrow V$ une dérivation.*

Démonstration Soient $s : R \longrightarrow B$ une application et $a, b \in R$. Donc s s'écrit (ψ, D) avec $\psi : R \longrightarrow A$ et $D : R \longrightarrow V$ des fonctions et on a les identités :

$$s(a)s(b) = (\psi(a)\psi(b), \psi(a)D(b) + \psi(b)D(a))$$

$$s(ab) = (\psi(ab), D(ab))$$

Donc s est un morphisme si et seulement si ψ est un morphisme et D une dérivation.

On suppose maintenant que A est une algèbre de Hopf de comultiplication M représentant un schéma en groupe affine E. Soit R une algèbre de Hopf représentant un schéma en groupe affine F. Sur $G = G_R = Hom(R, A \oplus V)$ on définit une loi de groupe par :

$$(\psi_1, D_1)(\psi_2, D_2) = (\psi_1\psi_2, \psi_1 D_2 + \psi_2 D_1)$$

avec $\psi_1\psi_2$ le produit dans $F(A)$ et pour tout $a \in R$:

$$\psi_1 D_2(a) = \sum_\alpha \psi_1(a_\alpha) D_2(b_\alpha)$$

avec $\sum_\alpha a_\alpha \otimes b_\alpha$ la comultiplication de a. Nous identifions $F(A)$ avec le groupe

$$\{(\psi, 0) | \psi \in F(A)\}$$

Lemme 31 *Le groupe G est produit semi-direct du groupe $F(A)$ et du sous-groupe normal :*

$$N = \{(\varepsilon, D) | D \in D(A, V)\}$$

Démonstration On considère le morphisme Φ de G vers $F(A)$ qui à (ψ, D) associe $(\psi, 0)$. Alors la restriction de Φ à $F(A)$ est l'indentité et en reamrquant que $(\varepsilon, 0)$ est l'élément neutre de G, on a $ker(\Phi) = N$.

Lemme 32 *Si I est le noyau de l'augmentation de A et $M(a) = \sum_\alpha a_\alpha \otimes b_\alpha$ pour a un élément de A alors $\Omega_A \cong A \otimes I/I^2$ et la dérivation universelle $d_0 : A \longrightarrow \Omega_A$ est donné par la formule :*

$$d_0(a) = \sum_\alpha a_\alpha \otimes d(b_\alpha)$$

avec $d : A \longrightarrow I/I^2$ le morphisme qui à $c + \xi \in A \cong K \otimes I$ associe ξ mod I^2.

Démonstration Notons 1 l'identité sur A alors la bijection :

$$G_A \ni (\varepsilon, D) \longmapsto (1, 0)(\varepsilon, D) = (1, 1.D) \in G_A$$

induit une autre bijection des dérivations de A vers V_ε (où V_ε est le module V sur A par le biais de ε) vers les dérivations de A vers V. Or :

$$D(A, V_\varepsilon) \cong Hom_K(I/I^2, V) \cong Hom_A(A \otimes_K I/I^2, V)$$

dont la dérivation universelle T est définie par $T(a) = 1 \otimes d(a)$ pour tout $a \in A$ avec $d : A \longrightarrow I/I^2$ la dérivation de l'énoncé. Donc $d_0 = 1.T$ est la dérivation cherchée.

Lemme 33 *I/I^2 est un espace vectoriel de dimension finie sur K.*

Démonstration Tout d'abord puisque A est noethérien, I est engendré par un nombre fini d'eléments $a_1, a_2, ..., a_n$. Notons $\pi : I \longrightarrow I/I^2$ le morphisme de passage aux quotients et ξ mod I^2 un élément de I/I^2 donc il existe des éléments $(b_1, u_1)..., (b_n, u_n)$ de $I \times K$ tels que :

$$\xi = (b_1 + u_1)a_1 + (b_2 + u_2)a_2 + ... + (b_n + u_n)a_n$$

Donc en appliquant π, il s'ensuit :

$$\pi(\xi) = u_1\pi(a_1) + u_2\pi(a_2) + ... + u_n\pi(a_n)$$

et donc I/I^2 est engendré sur K par $\pi(a_1), ..., \pi(a_n)$.

Le résultat suivant est le théorème de Cartier

Théorème 23 *Toute algébre de Hopf de type fini sur un corps de caractéristique nulle est réduite.*

Démonstration

Corollaire 12 *En caractéristique nulle, tout schéma en groupe affine fini sur un corps est étale.*

2.3 Schémas en groupe affine fini plat et quotient

Soient E, F des schémas en groupe algébriques sur un corps K représentés par des algèbres A et B.

Définition Un morphisme de $\psi : E \longrightarrow F$ est un quotient si le morphisme de B vers A induit par ψ est injectif.

Proposition 54 *Tout morphisme $f : E \longrightarrow F$ se factorise en une suite de morphismes*

$$E \xrightarrow{\pi} T \xrightarrow{g} F$$

avec $\pi : E \longrightarrow T$ un quotient et $g : T \longrightarrow F$ une immersion fermée.

Démonstration Soit $u : B \longrightarrow A$ le morphisme induit par f. Alors u se factrorise en :

$$B \xrightarrow{p} B/I \xrightarrow{\overline{u}} A$$

Or on a déjà vu que B/I est une algébre de Hopf et on note T le schéma en groupe affine représenté par B/I. Donc la suite précédente induit les morphismes voulus.

Pour aller plus dans l'etude des morphismes quotients nous devons faire un préliminaire sur les modules plats.

2.3.1 Module plat

Soit A un anneau. La nomenclature suivante est dû à Jean-Pierre Serre :

Définition Un module V sur A est dit plat ou tensoriellement exact si pour toute injection

$$\{0\} \longrightarrow W \longrightarrow T$$

de modules sur A, la suite

$$\{0\} \longrightarrow W \otimes V \longrightarrow T \otimes V$$

est exacte.

Proposition 55 *Si S est une partie multiplicative de A alors $S^{-1}A$ est un module plat sur A.*

Démonstration Soit

$$\{0\} \longrightarrow W \xrightarrow{\psi} T$$

une injection. Supposons que :

$$\psi(v_1) \otimes \frac{a_1}{s_1} + \psi(v_2) \otimes \frac{a_2}{s_2} + ... + \psi(v_n) \otimes \frac{a_n}{s_n} = 0$$

avec $v_i \in W$, $a_i \in A$ et $s_i \in S$ avec $i = 1, 2, ..., n$. Comme $W \otimes S^{-1}A \cong S^{-1}W$, cela implique :

$$\frac{\psi(v_1)}{s_1} a_1 + \frac{\psi(v_2)}{s_2} a_2 + ... + \frac{\psi(v_n)}{s_n} a_n = 0$$

Ensuite, en réduisant au même dénominateur, on obtient une expression de la forme : $\psi(v)/s = 0$ avec $v \in W$ et $s \in S$. Donc il existe $u \in S$ tel que $\psi(uv) = 0$ soit $uv = 0$. Il s'ensuit $v/s = 0$ et finalement :

$$v_1 \otimes \frac{a_1}{s_1} + v_2 \otimes \frac{a_2}{s_2} + ... + v_n \otimes \frac{a_n}{s_n} = 0$$

ce qui montre notre résultat.

Soit V une algèbre plate sur A.

Définition V est dite pleinement plate si le morphisme $T \longrightarrow T \otimes V$ envoyant $v \in T$ vers $v \otimes 1$ est injectif pour tout module T sur A.

Proposition 56 *Les conditions suivantes sont équivalentes.*
$(PP1)$ *V est pleinement plate.*
$(PP2)$ *Pour tout module T sur A, $T \otimes V = \{0\}$ alors $T = \{0\}$.*
$(PP3)$ *Si $\psi : T_1 \otimes V \longrightarrow T_2 \otimes V$ est un morphisme injectif induit par un morphisme u de modules sur A entre T_1 et T_2 alors u est injectif.*

Démonstration Montrons que $(PP2)$ implique $(PP3)$. On a l'injection

$$\{0\} \longrightarrow Ker(u) \longrightarrow T_1$$

Donc par platitude :

$$\{0\} \longrightarrow Ker(u) \otimes V \longrightarrow T_1 \otimes V$$

est exacte. En outre, $Ker(u) \otimes V$ est inclus dans $Ker(\psi) = \{0\}$. Enfin par $(PP2)$: $Ker(u) = \{0\}$. Montrons $(PP3)$ implique $(PP1)$. En effet, $T \otimes V \longrightarrow (T \otimes V) \otimes V$ est injectif puisque :

$$(T \otimes V) \otimes V \ni v \otimes a \otimes b \mapsto v \otimes ab \in T \otimes V$$

est un inverse. Donc par $(PP3)$: le morphisme $T \longrightarrow T \otimes V$ est injectif.

2.3.2 Quotient

2.3.3 Théorème de Lagrange

3 Application à la théorie des courbes elliptiques

3.1 Courbe elliptique en toute caractéristique

3.1.1 Equation de Weiertrass, discrimant et invariant modulaire

3.1.2 Loi de groupe et isogènie

3.1.3 Courbe elliptique sur les nombres complexes

4 Appendices

4.1 Introduction aux représentations linéaires de groupes finis

4.1.1 Définitions

Nous rappelons les rudiments de la théorie des représentations des groupes finis. L'idée est simple on veut faire apparaître les groupes finis comme quotient d'un sous-groupe fini d'automorphismes linéaires d'un espace vectoriel de dimension finie. Pour cela on définit une représentation comme un morphisme d'un groupe G vers les automorphismes $GL(E)$ avec E un espace vectoriel complexe de dimension égale à n. L'entier n étant appelé le degré de la représentation. Il est important de signaler que toutes nos représentations seront de degré fini. Ainsi si $\rho : G \longrightarrow GL(E)$ est une représentation, g un élément de G et v un vecteur de E alors on note

$$g.v = \rho(g)(v)$$

Ce qui laisse apparaître E comme un module sur l'algébre de groupes $\mathbb{C}[G]$. En effet, les axiomes de représentations sous cette nouvelle ecriture s'ecrivent :

$(R1)$ $g.(av + bw) = ag.v + bg.w$
$(R2)$ $g.(h.v) = (gh).v$
$(R3)$ $1.v = v$

Avec a, b des nombres complexes, g, h des éléments de G et v, w des vecteurs de E. Ainsi par abus nous désignons par E la représentation lorsque la mention de ρ est claire.

Définition Soit E une représentation d'un groupe fini G. Un sous-espace vectoriel F de E est une sous-représentation de E si pour tout élément g de G et tout vecteur v de F, $g.v$ appartient à F. Par conséquent, on vérifie que la restriction à F de la représentation de E sur G définit une représentation sur F.

Définition Soient E, F deux représntations d'un groupe fini G on appelle morphisme de représentations une application linéaire $f : E \longrightarrow F$ telle que pour tout vecteur $v \in E$ et tout $g \in G$, $f(g.v) = g.f(v)$.

Donnons des exemples :

Exemple 1 : Groupes cycliques Soit N un entier ≥ 1. On considère le morphisme de groupes de $\mathbb{Z}/N\mathbb{Z}$ vers $GL_2(\mathbb{C})$ qui tout entier n modulo N associe la matrice

$$M_n = \begin{pmatrix} \cos(\frac{2n\pi}{N}) & -\sin(\frac{2n\pi}{N}) \\ \sin(\frac{2n\pi}{N}) & \cos(\frac{2n\pi}{N}) \end{pmatrix}$$

On a ainsi une représentation en composant les fléches

$$\mathbb{Z}/N\mathbb{Z} \longrightarrow GL_2(\mathbb{C}) \longrightarrow GL(\mathbb{C}^2)$$

Le premier morphisme est déja décrit, le second fait correspondre à toute matrice M_n l'automorphisme linéaire de $\mathbb{C}^2$

$$(x,y) \longmapsto \begin{pmatrix} \cos(\frac{2n\pi}{N}) & -\sin(\frac{2n\pi}{N}) \\ \sin(\frac{2n\pi}{N}) & \cos(\frac{2n\pi}{N}) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Le lecteur aura remarqué que toutes ces matrices sont diagonalisables dans la même base puisque que le polynôme $X^n - 1$ les annule toutes et que chaque matrice M_n commute deux à deux entre elles.

Exemple 2 : Noyaux et images Soient E, F deux représentations d'une groupe fini G et $f : E \longrightarrow F$ un morphisme de représentations. En fait si E_0 est une représentation de F alors l'image $f(E_0)$ est une sous-representation de F. De même, si F_0 est une sous-représentation de F alors $f^{-1}(F_0)$ est une sous-représentation de E. En particulier, $Ker(f)$ et $Im(f)$ sont des sous-représentations respectives de E et F.

Exemple 3 : Représentation unitée Soit E une représentation sur un groupe fini G. On note E^G le sous-espace vectoriel invariant sous l'action de G, en d'autres termes les vecteurs de v de E^G vérifient $g.v = v$ pour tout $g \in G$. On vérifie que E^G est une sous-représentation de E. Par suite, on dit qu'une sous-représentation F de degré 1 l'unité si le morphisme $G \longrightarrow GL(F)$ est constant. Ainsi, on remarque que E^G est somme de représentations unitées.

Exemple 4 : Représentations duales Soient G un groupe fini et E, F deux représentations du groupe G. Nous allons maintenant parler de la représentation duale. Pour cela il nous faut définir une structure de réprésentation sur l'espace vectoriel complexe des applications linéaires de E vers F que nous dénotons par $Hom(E,F)$. Soit f un élément de $Hom(E,F)$ et $g \in G$, on note $g.f$ le morphisme de représentations défini par

$$g.f(v) = g.f(g^{-1}.v)$$

pour tout vecteur v de E. Par conséquent, si l'on désigne par E^* l'espace vectoriel dual de E alors on définit une structure de représentation sur E^* de la même manière sauf que la représentation $\mathbb{C}$ est muni de la représentation unité. De manière plus explicite, si l est une forme linéaire de E^*, on note pour tout $v \in E$

$$g.l(v) = l(g^{-1}.v)$$

Par ailleurs, on laisse le soin au lecteur de montrer que le sous-espace vectoriel des morphimes de représentations $Hom_G(E,F)$ est une sous-représentation égale à $Hom(E,F)^G$.

Exemple 5 : Représentation régulières Soit G un groupe fini et R l'espace vectoriel sur $\mathbb{C}$ engendré par une base $(e_g)_{g\in G}$ indéxée sur les éléments de G. Donc si $v \in R$ alors v s'écrit

$$v = \sum_{g\in G} a_g e_g$$

avec a_g des nombres complexes pour tout $g \in G$. Soit $h \in G$. Donc on définit une représentation R en posant

$$h.v = \sum_{g\in G} a_g e_{hg}$$

Cette représentation R est appelée représentation régulière.

La catégorie des repésentations d'un groupe fini G est en fait additive :

Définition Soient E, F des représentations d'un groupe G. On définit une structure de représentations sur $E \oplus F$ et $E \otimes F$ de la manière suivante. Pour tout $g \in G$ et tous vecteurs $v \in E$ et $w \in F$, on a

$$g.(v \oplus w) = g.v \oplus g.w$$

$$g.(v \otimes w) = g.v \otimes g.w$$

Par abus, nous appelons supplémentaire d'une sous représentation E_1 de E, une sous-représentation E_2 telle que $E = E_1 \oplus E_2$.

4.1.2 Représentations irréductibles

Nous avons maintenant les moyens pour aller dans le vif du sujet. Nous commençons par une proposition qui se déduit des remarques de la sous-section précédente. Comme précédemment, nous précisons que toutes nos représentations sont complexes, de degrés finis et sur un groupe fini. On invite le lecteur à verifier où ces hypothèses sont utilisées dans les résultats qui vont suivre.

Proposition 57 *Toute sous-représentation admet un supplémentaire.*

Démonstration Soit E une représentation et E_0 une sous-représentation. On considère une projection linéaire $p : E \longrightarrow E$ sur E_0. Alors l'application linéaire f définit par

$$f(v) = \frac{1}{|G|} \sum_{g\in G} (g.p)(v)$$

pour tout vecteur $v \in E$ est encore une projection linéaire et est un morphisme de représentations. Donc $Ker(f)$ est un supplémentaire de la sous-représentation E_0.

La définition suivante est importante :

Définition Une sous-représentation E est dite irréductible si ces seules sous-représentations sont exactement $\{0\}$ ou E. On convient que la sous-représentation nulle n'est pas irréductible.

Exemple 1 : La dimension 1 Les représentations de dimension un sont irréductibles. On remarque que le groupe des inversibles $\mathbb{C}^\times$ s'identifie naturellement à $GL(\mathbb{C})$ par l'application qui à tout nombre complexe a non nul associe l'homothétie $z \longmapsto az$. Ainsi l'etude des représentions de degré 1 d'un groupe fini G se limite à celle des morphismes de groupes $Hom(G, \mathbb{C}^\times)$ de G vers $\mathbb{C}^\times$. On observe que $Hom(G, \mathbb{C}^\times)$ est muni d'une structure de groupe, on l'appelle le groupe dual, et que si $G = \mathbb{Z}/N\mathbb{Z}$ alors G est isomorphe à son dual. Par conséquent, en étudiant le comportement du dual avec le produit direct, on en déduit que tout groupe abélien est isomorphe à son dual.

Exemple 2 : Permutations Soit E un espace vectoriel de dimension N. Soient $e_1, e_2, ..., e_N$ les vecteurs de base de E. Alors tout vecteurs de E s'ecrit comme une combinaison linéaire

$$a_1e_1 + a_2e_2 + ... + a_{N-1}e_{N-1} + a_Ne_N$$

avec $a_1, a_2, ..., a_N$ des nombres complexes. Si σ est une permutation de $\mathfrak{S}_N$ alors on définit une représentation en spécifiant à l'expression ci-desssus le vecteur

$$a_1e_{\sigma(1)} + a_2e_{\sigma(2)} + ... + a_{N-1}e_{\sigma(N-1)} + a_Ne_{\sigma(N)}$$

Soit F le sous-espace vectoriels formé des vecteurs dont la sommes des composantes le long de $e_1, e_2, ..., e_N$ est nulle. On verifie que F est une sous-représentation de E. On peut montrer à l'aide de la théorie des caractère que F est une sous-représentation irréductible.

Le lemme dit de Schur est essentiel dans la théorie des modules décomposables

Lemme 34 *Soient E, F deux sous-représentations irréductibles. Alors la dimension de $Hom_G(E, F)$ est un élément de $\{0, 1\}$, si cette dernière est non nulle alors il existe un isomorphisme de représentations $f : E \longrightarrow F$ telle que $Hom_G(E, F)$ soit égales $\mathbb{C}f$.*

Démonstration Soit $f : E \longrightarrow F$ un morphisme de représentations non nul. Alors $Ker(f)$ et $Im(f)$ sont égaux respectivement à $\{0_E\}$ et F par irreductibilité. Donc f est un isomorphisme. Soit g un autre morphisme de représentations de E vers F. Alors par le raisonnement précédent g est un isomorphisme. Puisque que le corps de base est le corps des complexes, il existe une valeur propre $a \in \mathbb{C}$ de $g^{-1} \circ f$. Donc son sous-espace propre est une sous-représentation de E. Donc par définition de a et par irrédutibilité de E, on obtient $g^{-1} \circ f = a.1$, soit $f = ag$.

Théorème 24 *Toute représention E isomorphe à une somme directe d'un nombre fini de sous-repreésentations irréductbles. En outre si on a deux décompositions en irréductibles*

$$E \cong \bigoplus_{i=1}^{N} E_i^{\oplus n_i}$$

$$E \cong \bigoplus_{i=1}^{M} F_i^{\oplus m_i}$$

alors $N = M$ et il existe une permutation σ de $\mathfrak{S}_N$ telle que $E_i \cong F_{\sigma(i)}$ et $n_i = m_{\sigma(i)}$ pour tout entier $i = 1, 2, ..., N$.

Démonstration Soient j, k des entiers compris entre 1 et N. Tout d'abord, supposons que deux telles décompositions existent. Donc en utilisant le lemme de Schur, si $E_j \cong F_k$ alors

$$n_j = dim[Hom_G(E, E_j)] = dim[Hom_G(E, F_k)] = m_k$$

et $N = M$. Il reste à montrer l'existence. On raisonne par récurrence. Si le degré de E, disons n, est égal à 1 alors E est irréductible. Supposons le résultat vrai pour un entier $n \geq 1$. Soit F une sous-représentation propre de E. Alors d'aprés la proposition précédente, il existe un supplémentaire H de F. Ensuite on décompose F et H en somme d'irréductibles par l'hypothèse de récurence. Enfin, on conclut en regroupant les deux sommes.

4.1.3 Caractères

Nous allons maintenant définir un invariant numérique de classes d'isomorphie des représentations irreductibles. Nous rappelons que toutes nos représentations sont de degré fini.

Définition Soient G un groupe fini et $\rho : G \longrightarrow E$ une représentation. On appelle caractére de la représentation E l'application qui à tout élément g de G associe la trace $\chi_E(g)$ de l'automorphisme linéaire $\rho(g)$.

En fait, les caractéres sont un cas particulier de fonctions centrales.

Définition On appelle fonction centrale sur G toute fonction de G vers les nombres complexes $\mathbb{C}$ constante sur les classes de conjugaison de G.

L'ensemble de toutes les fonctions centrales sur G est un espace vectoriel complexe de dimension égale le nombre de classes de conjugaison de G, on le dénote par $F(G) = F_{\mathbb{C}}(G)$. La proposition ci-dessus se déduit en utilisant des bases de diagonalisations pour les automorphismes images des représentations E et F. Notons tout de même que si $e_1, e_2, ..., e_N$ et $f_1, f_2, ..., f_M$ sont des vecteurs de bases repectifs de E et F alors $e_i \otimes f_j$ pour $i = 1, 2, ..., N$ et $j = 1, 2, ..., M$ sont des vecteurs de base de $E \otimes F$. Enfin, puisque $E \otimes F = Hom(E^*, F)$, il s'ensuit que $Hom(E, F)$ est isomorphe à $E^* \otimes F$.

Proposition 58 *Si E, F sont deux représentations alors on a les régles*
$(C1)$ $\chi_{E\oplus F} = \chi_E + \chi_F$
$(C2)$ $\chi_{E\otimes F} = \chi_E \chi_F$
$(C3)$ $\chi_{E^*} = \overline{\chi_E}$
$(C4)$ $\chi_{Hom(E,F)} = \overline{\chi_E}\chi_F$

Démonstration Par les remarques précédentes, on a $(C1)$ et $(C2)$. Ensuite, si l'on suppose $(C3)$ alors on obtient $(C4)$ par $(C2)$. Il reste donc à démontrer $(C3)$. Notons $\rho : G \longrightarrow GL(E)$ la représentation E. Soient n le cardinal de G, $g \in G$ et $(e_1, e_2, ..., e_N)$ une base de diagonalisation de $\rho(g)$ de valeurs propres $\zeta_1, \zeta_2, ..., \zeta_N$. Puisque tout élement de g de G verifie $g^n = 1$, on observe que ζ_i est une racine $n-$ième de l'unité pour tout $i = 1, 2, ..., N$. Ensuite l'image de g par la représentation duale est $\rho(g^{-1})^T$ et donc la matrice de celle-ci dans la base ci-dessus est une matrice diagonale dont les valeurs propres sont les inverses des ζ_i. Enfin, on conclut en remarquant que l'inverse d'une racine à l'unité est sa conjuguée.

Théorème 25 *Si E est une représentation d'un groupe fini G alors la dimension de E^G est égale à*

$$\frac{1}{|G|}\sum_{g\in G}\chi_E(g)$$

Démonstration Soit $p : E \longrightarrow E$ une projection linéaire sur E^G. Si $v \in E$ alors

$$f(v) = \frac{1}{|G|}\sum_{g\in G}(g.p)(v) = \frac{1}{|G|}\sum_{g\in G} g.v$$

Soit s la dimension de E^G et $e_1, e_2, ..., e_s$ des vecteurs bases de E^G. Ainsi on compléte celle-ci avec une base de $Ker(f)$, on obtient une base $(e_1, e_2, ..., e_N)$ de E dont la matrice de l'endomorphisme f dans cette dernière base est donnée par une matrice de la forme

$$\begin{pmatrix} I_s & 0 \\ 0 & 0 \end{pmatrix}$$

avec I_s la matrice identité de taille $s \times s$. Donc en calculant la trace :

$$dim(E^G) = tr(f) = \frac{1}{|G|} \sum_{g \in G} \chi_E(g)$$

Définition Soient α, β deux fonctions centrales de $F(G)$. On note

$$(\alpha, \beta) = \frac{1}{|G|} \sum_{g \in G} \overline{\alpha(g)} \beta(g)$$

Cela définit un produit scalaire sur l'espace des fonctions centrales $F(G)$.

En remarquant que $Hom_G(E, F) = Hom(E, F)^G$, on obtient :

Corollaire 13 *Soient E, F deux représentations d'un groupe fini G alors la dimension de $Hom_G(E, F)$ est égale à (χ_E, χ_F).*

Soient $E_1, E_2, ..., E_M$ des représentants de classes d'isormorphie des représentations irréductibles. Par abus de langage, nous les appelons les représentations irréductibles de G et nous appelons caractères irréductibles, les caractères $\chi_{E_1}, \chi_{E_2}, ..., \chi_{E_M}$. En appliquant le corollaire précédent et le lemme de Schur, il s'ensuit que :

Corollaire 14 *Les caractères irréductibles forment une famille orthonormée pour le produit scalaire des fonctions centrales.*

En particulier, le nombre de caractère irréductible est inférieur au nombre de classes de conjuguaison de G.

Définition Soient α une fonction centrale et χ_E un caractère d'une représentation E. On appelle transformée de Fourier de α la fonction $\hat{\alpha}$ définie sur les caractères de représentations par

$$\hat{\alpha}(\chi_E) = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \overline{\alpha}(g) \chi_E(g)$$

On observe qu'avec les mêmes notations que ci-dessus, $\hat{\alpha}(\chi_E)$ est en fait le caractère de la représentation E, de l'endomorphisme de représentations qui à tout élément $g \in G$ associe

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} \overline{\alpha}(g) \rho_E(g)$$

où on dénote par ρ_E la représentation E.

En fait, on peut dire mieux que le corollaire précédent :

Théorème 26 *Les caractères forment une base orthonormée des fonctions centrales.*

Démonstration Soit α une fonction centrale. Il s'agit de montrer que si pour tout caractère irréductible χ_F on a $(\alpha, \chi_F) = 0$ alors $\alpha = 0$. Soit F une représentation irréductible. On observe que

$$f_F = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \overline{\alpha}(g) \rho_F(g)$$

est un endomorphisme de représentations de F. Donc par le lemme de Schur, f_F est une homothétie. Donc en calculant la trace de f_F, on obtient

$$tr(f_F) = \frac{1}{\sqrt{|G|}} (\alpha, \chi_F) = 0$$

Donc f_F est nulle. Ensuite si E est une représentation alors E est isomorphe à une somme représentations irréductibles, disons $F_1, F_2, ..., F_M$ et

$$f_E = f_{F_1} + f_{F_2} + ... + f_{F_M} = 0$$

Donc en choisissant $E = R$ la représentation régulière, il vient

$$f_R = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \overline{\alpha}(g) e_g = 0$$

Or $(e_g)_{g \in G}$ est une base, donc $\overline{\alpha}(g) = 0$, pour tout $g \in G$. Donc $\alpha = 0$.

Donc le théorème nous dit que le nombre de classes de congugaison est égal au nombre de représentations irréductibles de G. En particulier, nous avons remarqué précédemment que les représentations irréductibles d'un groupe abélien s'identifiaient avec son groupe dual qui est de même cardinal que celui-ci. Ainsi toutes les représentations d'un groupe abélien sont de dimension 1. Enfin, nous définissons un invariant important dans la classification des groupes finis :

Définition Soit G un groupe fini et $\chi_1, \chi_2, ..., \chi_N$ les caractères irréductibles et $g_1, g_2, ..., g_N$ des représentants des différentes classes de conjugaison de G. On appelle table de caractère de G, la matrice carrée $(\chi_i(g_j))_{1 \leq i,j \leq N}$.

4.2 Modules

Le but de cette appendice est de compléter nos connaissance sur les modules.

4.2.1 Modules projectifs

Soit B un anneau. Dans notre contexte le mot suite désigne une suite de morphismes de modules sur B.

Nous rappelons qu'une suite

$$... \longrightarrow V_i \stackrel{\psi_i}{\longrightarrow} V_{i+1} \stackrel{\psi_{i+1}}{\longrightarrow} V_{i+2} \longrightarrow ...$$

est un complexe si $Im(\psi_i) \subset Ker(\psi_{i+1})$ pour entier i et qu'elle est exacte si les inclusions sont des égalités. Ainsi, $u : V \longrightarrow W$ et $v : V \longrightarrow W$ sont respectivement injectif et surjectif si les suites :

$$\{0\} \longrightarrow V \stackrel{u}{\longrightarrow} W$$

$$V \stackrel{v}{\longrightarrow} W \longrightarrow \{0\}$$

sont exactes.

Proposition 59 *Soit*

$$\{0\} \longrightarrow V_1 \stackrel{\psi_1}{\longrightarrow} V_2 \stackrel{\psi_2}{\longrightarrow} V_3 \longrightarrow \{0\}$$

une suite exacte alors $(SC1)$ *: il existe un morphisme* $s : V_2 \longrightarrow V_3$ *tel que* $\psi_2 \circ s = id$ *si et seulement si* $(SC2)$ *: il existe un morphisme* $r : V_2 \longrightarrow V_1$ *tel que* $r \circ \psi_1 = id$*.*

Lorsque que une suite exacte courte comme ci-dessus vérifie $(SC1)$ ou $(SC2)$ on dit qu'elle est scindée.

Démonstration Supposons que l'on ait simultanément $(SC1)$ et $(SC2)$. Alors le morphisme sur son image :

$$\phi : V_2 \ni x \longmapsto (s \circ \psi_2(x), \psi_1 \circ r(x)) \in V \oplus W$$

est un isomorphisme. En effet, comme r et s sont respectivement surjectif et injectif, on a $V = s(Im(\psi_2)) \cong Im(\psi_2)$ et $W = Im(\psi_1) = Ker(\psi_2)$. Par ailleurs, supposons que l'on ait seulement $(SC1)$ alors pour tout $x \in V_2$ on pose pour r :

$$\psi_1 \circ r(x) = x - s \circ \psi_2(x)$$

r est bien définie puisque ψ_1 est injectif. Donc par exactitude :

$$\psi_1 \circ r \circ \psi_1(x) = \psi_1(x) - s \circ \psi_2 \circ \psi_1(x) = \psi_1(x)$$

et par injectivité de ψ_1 :

$$r \circ \psi_1(x) = x$$

L'implication inverse utilise des raisonnements analogues.

Définition On dit qu'un module V sur B est projectif si toute suite

$$\{0\} \longrightarrow V_1 \longrightarrow V_2 \longrightarrow V \longrightarrow \{0\}$$

exacte est scindée.

Soit F un foncteur de la catégorie des modules sur B vers celle des groupes abéliens. On dit que F est exacte si étant donné une suite

$$... \longrightarrow V_i \xrightarrow{\psi_i} V_{i+1} \xrightarrow{\psi_{i+1}} V_{i+2} \longrightarrow ...$$

exacte, la suite

$$... \longrightarrow F(V_i) \xrightarrow{\psi_i} F(V_{i+1}) \xrightarrow{\psi_{i+1}} F(V_{i+2}) \longrightarrow ...$$

est exacte.

Voici diverses caractérisations des modules projectifs qui sont laissées aux lecteurs

Proposition 60 *Soit V un module sur B. Alors les conditions suivantes sont équivalentes*
$(P1)$ *V est un module projectif.*
$(P2)$ *Le foncteur $W \longmapsto Hom(V, W)$ est exacte.*
$(P3)$ *Il existe un module Z tel que $V \oplus Z$ soit libre*
$(P4)$ *Si $\psi : V \longrightarrow W$ et $\pi : V \longrightarrow Z$ sont des morphismes de modules sur B avec π surjectif alors il existe un morphisme $u : V \longrightarrow Z$ tel que : $\pi \circ u = \psi$.*

Par $(P3)$ on remarque tout module libre est projectif.

4.2.2 Modules plats