Représentations en caractéristique positive et cohomologie

Pierre Guillot

19 novembre 2014

Bibliographie

[Alp86] J. L. Alperin, *Local representation theory*, Cambridge Studies in Advanced Mathematics, vol. 11, Cambridge University Press, Cambridge, 1986. MR 860771 (87i :20002)

[Bum98] Daniel Bump, *Algebraic geometry*, World Scientific Publishing Co., Inc., River Edge, NJ, 1998. MR 1669884 (2000a :14001)

[Car] Jon F. Carlson, *Cohomology and representation theory*, disponible en ligne.

[CTVEZ03] Jon F. Carlson, Lisa Townsley, Luis Valeri-Elizondo, and Mucheng Zhang, *Cohomology rings of finite groups*, Algebras and Applications, vol. 3, Kluwer Academic Publishers, Dordrecht, 2003. MR 2028960 (2004k :20110)

Dans cette partie du cours nous allons essentiellement présenter les parties les plus accessibles de l'article de Carlson [Car]. Cet article est lui-même une introduction à la lecture du livre [CTVEZ03], qui est très complet. On notera que la lecture du livre n'est pas plus difficile que celle de l'article, au contraire même puisque tous les détails sont donnés tranquillement ; mais par contre c'est un très gros ouvrage pour lequel il faut avoir du temps.

Nous utiliserons [Alp86], de Alperin, comme référence pour les représentations en caractéristique positive. Le petit livre de Bump [Bum98] pourra être consulté pour les rares références à la géométrie algébrique que nous ferons.

Les trois livres cités sont à la bibliothèque de l'IRMA.

Table des matières

Chapitre 1

Introduction & Généralités

Nous allons nous intéresser aux représentations d'un groupe fini sur un corps k quelconque. Dès que cela simplifiera les choses, nous supposerons que k est algébriquement clos, et nous éviterons ainsi les difficultés dans cette direction. Par contre on ne va pas supposer que k est de caractéristique nulle. La lettre p va toujours désigner un nombre premier, qui sera souvent la caractéristique de k.

§1. Les corps finis

Faisons quelques rappels.

Lemme 1.1.1. *Pour chaque entier $r \geq 1$ il existe un corps fini possédant p^r éléments, unique à isomorphisme (non canonique) près. On le note $\mathbf{F}_{p^r}$.*

Démonstration. Le corps $\mathbf{Z}/p\mathbf{Z}$ répond à la question dans le cas $n = 1$. Si K est un corps à p^r éléments, alors il contient $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$. Le groupe multiplicatif $K^\times$ des éléments non nuls est d'ordre $p^r - 1$, donc si $x \neq 0$ on a $x^{p^r-1} = 1$, d'où finalement $x^{p^r} - x = 0$ pour tout $x \in K$.

Ainsi K doit être le corps obtenu en ajoutant à $\mathbf{F}_p$ les racines du polynôme $P = X^{p^r} - X$ (et les éléments de K constituent même *toutes* les racines de ce P). Ceci établit l'unicité (cf cours de théorie des corps).

Pour l'existence, pas le choix : on pose $\mathbf{F}_{p^r}$ = le corps obtenu en rajoutant à $\mathbf{F}_p$ les racines de P (on sait que ceci a un sens, cf même cours). Puisque $P' = -1$, le polynôme P n'a pas de racines doubles, ou autrement dit il en possède p^r distinctes. Soit K l'ensemble de ces racines : on a $K \subset \mathbf{F}_{p^r}$, et momentanément on se demande si $K = \mathbf{F}_{p^r}$. Pour vérifier ceci il suffit de montrer que K est un corps, et à vrai dire on vérifie immédiatement que si $x, y \in K$ alors $x + y \in K$, $xy \in K$ et $x^{-1} \in K$. Donc $K = \mathbf{F}_{q^r}$ et ce corps possède bien p^r éléments. □

Notons qu'un corps de caractéristique p est un espace vectoriel sur $\mathbf{F}_p$, et s'il est fini il doit être de dimension finie, donc isomorphe à $(\mathbf{F}_p)^r$ et d'ordre p^r. On a donc décrit tous les corps finis. Notons aussi :

Lemme 1.1.2. *Un corps fini n'est jamais algébriquement clos.*

Démonstration. Si $K = \{x_1, \ldots, x_m\}$ alors le polynôme

$$P = (X - x_1) \cdots (X - x_m) + 1$$

n'a pas de racines dans K. □

On notera $\overline{\mathbf{F}}_p$ la clôture algébrique de $\mathbf{F}_p$. On sait qu'elle existe et qu'elle est unique à isomorphisme près. Lorsque $x \in \overline{\mathbf{F}}_p$, le corps $\mathbf{F}_p(x)$ est de dimension finie sur $\mathbf{F}_p$, donc il est fini et c'est l'un des $\mathbf{F}_{p^r}$ pour un certain r. On peut donc penser à $\overline{\mathbf{F}}_p$ comme à la réunion de tous les $\mathbf{F}_{p^r}$.

Voici enfin un petit résultat sur le groupe des matrices inversibles à coefficients dans $\mathbf{F}_q$, où $q = p^r$.

Lemme 1.1.3. *Le groupe $GL_n(\mathbf{F}_q)$ est d'ordre $(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})$. Le sous-groupe des matrices triangulaires supérieures avec uniquement des 1 sur la diagonale est un p-sous-groupe de Sylow.*

Démonstration. Voici une méthode pour construire une matrice inversible à coefficients dans $\mathbf{F}_q$: vous vérifierez que l'on obtient chaque matrice une fois et une seule de cette façon.

On choisit d'abord le vecteur v_1 dont les coordonnées dans la base canonique de $\mathbf{F}_q^n$ vont former la première ligne de la matrice. On le prend quelconque mais non-nul (sinon le déterminant s'annulerait), ce qui laisse $q^n - 1$ choix.

Puis on choisit v_2 tel que v_1, v_2 soit libre, c'est-à-dire que v_2 ne doit pas être sur la droite engendrée par v_1 qui comporte q éléments. Ceci laisse $q^n - q$ choix.

Ainsi de suite, si $v_1, \ldots, v_k$ on été choisis, on prend v_{k+1} de sorte qu'il n'appartienne pas à l'espace engendré par les autres v_i, qui est de dimension k par construction et possède donc q^k éléments : $q^n - q^k$ choix s'offrent à nous. On continue jusqu'à n et le nombre de choix que l'on a eus est bien celui annoncé.

Écrivons $q^n - q^k = q^k(q^{n-k} - 1)$ et remarquons que $(q^{n-k} - 1)$ est premier à p. On en déduit que l'ordre de $GL_n(\mathbf{F}_q)$ est de la forme

$$q^{1+2+\cdots+(n-1)}m = q^{\frac{n(n-1)}{2}}m$$

où m est premier à p. Un p-groupe de Sylow de ce groupe est alors un sous-groupe d'ordre $q^{\frac{n(n-1)}{2}}$.

Pour le sous-groupe proposé, on est entièrement libre de choisir les coefficients au-dessus de la diagonale. Il y a q choix pour chaque emplacement, et $n-1$ choix à faire sur la première ligne, $n-2$ sur la deuxième, etc, donc en tout le nombre d'éléments dans ce sous-groupe est bel et bien $q^{\frac{n(n-1)}{2}}$. □

§2. Modules semi-simples

On prend un groupe fini G et un corps k quelconque. L'exemple à garder en tête est $k = \overline{\mathbf{F}}_p$, mais au début on procède de façon générale. Un G-module sur k, ou une représentation de G sur k, est (comme vous le savez) un espace vectoriel sur k, disons V, muni d'un homomorphisme $\rho\colon G \to GL(V)$. Il revient au même d'exiger que l'on ait une application $G \times V \longrightarrow V$, notée $(g, v) \mapsto g \cdot v$ ou même gv, telle que $v \mapsto g \cdot v$ est linéaire (c'est l'application $\rho(g)$), et de sorte que $g \cdot (h \cdot v) = (gh) \cdot v$ (ce qui traduit que ρ est un homomorphisme). Un isomorphisme entre deux G-modules V et W est une application linéaire $\phi\colon V \to W$ telle que $\phi(gv) = g\phi(v)$.

On dira qu'un G-module V est *simple*, ou *irréductible*, lorsque ses seuls sous-modules sont V lui-même et $\{0\}$.

Un exemple tout bête de module simple est ce qu'on appelle le « module trivial » : il s'agit du corps k, comme espace vectoriel sur lui-même, avec $g \cdot x = x$ pour tous $g \in G$, $x \in k$. Le résultat suivant devrait vous frapper.

Proposition 1.2.1. *Soit G un p-groupe, et soit $k = \mathbf{F}_{p^r}$ un corps fini de caractéristique p. Alors le seul module simple de G est le module trivial. De plus, ceci est encore vrai avec $k = \overline{\mathbf{F}}_p$.*

Démonstration. Soit $G' = \rho(G)$, l'image de G par l'homomorphisme ρ correspondant à un module simple V. Alors G' est un p-groupe, tout comme G.

Soit S le sous-groupe de Sylow de $GL_n(\mathbf{F}_{p^r})$ décrit dans le lemme 1.1.3. Les théorèmes de Sylow garantissent que l'on peut conjuguer G' en un sous-groupe de S ; en clair, il existe $A \in GL_n(\mathbf{F}_{p^r})$ telle que $A^{-1}G'A \subset S$, ou encore $G' \subset ASA^{-1}$.

Les matrices dans S fixent toutes le premier vecteur de la base canonique. Les matrices dans ASA^{-1}, en particulier toutes les matrices $\rho(g)$, fixent donc toutes le vecteur v donné par la première colonne de A.

Ainsi le vecteur $v \in V$ engendre un sous-espace de V qui est isomorphe au module trivial. Comme V est supposé simple, ce sous-module qui est non-nul doit être V tout entier. Voilà qui achève la démonstration dans le cas $k = \mathbf{F}_{p^r}$.

Pour traiter le cas $k = \overline{\mathbf{F}}_p$, on fait les remarques suivantes : on prend une base pour V de sorte que ρ est un homomorphisme $G \to GL_n(k)$; chaque coefficient de chaque matrice $\rho(g)$ est dans $\overline{\mathbf{F}}_p$, et appartient donc à un corps fini contenant $\mathbf{F}_p$ (cf une remarque plus haut). En prenant le plus petit corps K

contenant tous ces corps finis (et il n'y en a qu'un nombre fini en considération), on constate que K est lui-même fini, et on a en fait une factorisation

$$\rho\colon G \longrightarrow GL_n(K) \longrightarrow GL_n(\overline{\mathbf{F}}_p)\,,$$

et l'argument donné dans la première partie montre qu'il y a un $v \in V$ qui est fixé par tous les éléments de G. On conclut de la même manière. □

Voilà qui est bien différent du cas $k = \mathbf{C}$ que vous connaissez. Pour prolonger la discussion, on dit qu'un module est *semi-simple* lorsque c'est la somme directe de modules simples. Lorsque G est un p-groupe et que $k \subset \overline{\mathbf{F}}_p$, on voit donc qu'un module semi-simple V est une somme directe de copies du module trivial, ou en d'autres termes V est simplement un espace vectoriel avec l'action triviale $g \cdot v = v$ de G.

Rappelons que lorsque $k = \mathbf{C}$, *tous* les modules sont semi-simples. L'argument étant que si $U_1 \subset V$ est un sous-module (ce qui veut dire un sous-G-module, systématiquement), alors on peut trouver $U_2 \subset V$ un autre sous-module tel que $U_1 \oplus U_2 = V$, ce qui entraîne par récurrence immédiate que V est semi-simple. Rappelons aussi brièvement que pour montrer ceci, on part d'une projection quelconque $\pi\colon V \to U_1$ que l'on remplace ensuite par sa « moyenne » π_G :

$$\pi_G(v) = \frac{1}{|G|} \sum_{h \in G} \pi(h \cdot v)\,.$$

On vérifie que $\pi_G(gv) = g\pi_G(v)$, c'est-à-dire que π_G est un homomorphisme de G-modules $V \longrightarrow U_1$, puis que $\pi_G \circ \pi_G = \pi_G$ donc que c'est encore une projection. Le noyau $U_2 = \ker(\pi_G)$ convient alors.

Dans l'argument précédent, le point essentiel est simplement que l'on puisse diviser par $|G|$, l'ordre de G, et l'hypothèse minimale est donc que *la caractéristique de k ne divise pas $|G|$*.

Les modules semi-simples ont une propriété essentielle que l'on peut formuler à l'aide de $\mathrm{End}_G(V)$: par définition, pour tout module V, il s'agit de l'anneau (la k-algèbre, en fait) de tous les endomorphismes de V qui commutent avec l'action de G. On aura même besoin de parler de $\mathrm{Hom}_G(V, W)$, l'espace de toutes les applications linéaires $V \to W$ qui commutent avec l'action de G, de sorte que $\mathrm{End}_G(V) = \mathrm{Hom}_G(V, V)$.

Proposition 1.2.2. *1. Si V est un module simple, alors $\mathrm{End}_G(V)$ est un corps, qui est une extension finie de k. En particulier si k est algébriquement clos, alors $\mathrm{End}_G(V) = k$ dans ce cas.*

2. Si V et W sont deux modules simples qui ne sont pas isomorphes, alors $\mathrm{Hom}_G(V, W) = 0$.

3. Si V est un module semi-simple, alors $\mathrm{End}_G(V)$ est un produit d'algèbres de matrices sur différents corps, qui sont des extensions finies de k.

Les points (1) et (2) forment le « lemme de Schur ».

Démonstration. Soient V et W deux modules simples (non-nuls) de G, et soit $f \in \mathrm{Hom}_G(V,W)$. Alors $\ker(f)$ est un sous-module de V, c'est donc soit $\{0\}$ soit V. Si $\ker(f) = \{0\}$, alors W contient le sous-module $f(V)$ qui est isomorphe à V, et par simplicité de W on doit avoir $W = f(V)$. En particulier W est isomorphe à V dans ce cas. On a montré le (2) : en effet en excluant $V \cong W$, on exclut le cas $\ker(f) = \{0\}$ et on se retrouve avec $\ker(f) = V$ ou encore $f = 0$ pour tous les $f \in \mathrm{Hom}_G(V,W)$.

Mais essentiellement le (1) est montré aussi, en faisant $V = W$. En effet, on a établi qu'un élément de $\mathrm{End}_G(V)$ non-nul est un automorphisme de V, donc que les éléments non-nuls de l'anneau $\mathrm{End}_G(V)$ sont inversibles. C'est la définition d'un corps. Ce corps est contenu dans $\mathrm{End}(V)$ qui est de dimension finie sur k donc le reste est clair.

Passons au (3). Tout d'abord prenons le cas d'un module $U = S \oplus S \oplus \cdots \oplus S = S^n$ où S est simple, et soit $K = \mathrm{End}_G(S)$. Alors $\mathrm{End}_G(U) \cong M_n(K)$, comme on le voit en réfléchissant un peu. Maintenant considérons le cas $U = U_1 \oplus \cdots \oplus U_r$ où chaque U_i est comme précédemment (on dit parfois *isotypique*), c'est-à-dire $U_i = S_i^{n_i}$, et supposons que S_i n'est pas isomorphe à S_j lorsque $i \neq j$. Alors $\mathrm{Hom}_G(U_i, U_j) = 0$ par le (2). Il est alors clair que

$$\mathrm{End}_G(U) \cong \bigoplus_i M_{n_i}(K_i)\,,$$

avec $K_i = \mathrm{End}_G(S_i)$. □

Exemple 1.2.3. Nous allons examiner un module que l'on peut toujours définir, pour tout groupe G, et qui est particulièrement important. Il s'agit de la *représentation régulière*, notée kG ou $k[G]$.

On forme ce module en prenant un espace vectoriel avec une base en bijection avec les élements de G, de sorte que les vecteurs de kG peuvent se noter

$$\sum_{g \in G} \alpha_g\, g \qquad (*)$$

où α_g est un scalaire. Si l'on préfère, on peut dire que kG est l'ensemble des fonctions $G \longrightarrow k$, qui est naturellement un espace vectoriel, et que (*) est une notation suggestive pour désigner la fonction α telle que $\alpha(g) = \alpha_g$.

L'action de $\sigma \in G$ sur kG est donnée tout naturellement par

$$\sigma \cdot \left(\sum_{g \in G} \alpha_g\, g \right) = \sum_{g \in G} \alpha_g\, \sigma g = \sum_{g \in G} \alpha_{\sigma^{-1} g}\, g\,.$$

(Avec le point de vue « fonctions » c'est $(\sigma \cdot \alpha)(g) = \alpha(\sigma^{-1} g)$.)

On constate au moins que ce module est toujours non-trivial. Dans le cas où G est un p-groupe et $k \subset \overline{\mathbf{F}}_p$, ceci montre déjà que kG n'est pas semi-simple : les modules non-semi-simples existent bel et bien !

Mais il se trouve aussi que kG est un anneau. En fait il existe une unique multiplication sur kG qui prolonge le produit sur G, c'est-à-dire que l'on pose

$$\left(\sum_{g\in G} \alpha_g\, g\right)\left(\sum_{h\in G} \beta_h\, h\right) = \sum_{g,h\in G} \alpha_g\beta_h gh = \sum_{\sigma\in G}\left(\sum_{g,h \text{ tels que } gh=\sigma} \alpha_g\beta_h\right)\sigma\,.$$

On vérifie sans problème que cette formule donne bien un produit associatif, et donc un anneau (et même une algèbre sur k). Du point de vue « fonctions », c'est ce qu'on appelle le *produit de convolution* :

$$(\alpha\beta)(\sigma) = \left(\sum_{g,h \text{ tels que } gh=\sigma} \alpha(g)\beta(h)\right) = \sum_{g\in G} \alpha(g)\beta(g^{-1}\sigma)\,.$$

Ce qu'on constate immédiatement (surtout avec le premier point de vue – c'est moins clair avec les fonctions), c'est qu'un G-module, au sens où nous l'avons défini, est exactement la même chose qu'un module sur l'algèbre kG. Réfléchissez-y, on a tout fait pour !

Toute algèbre A peut être vue comme un module sur elle-même (c'est aussi bête que de dire que $\mathbf{R}$ est un $\mathbf{R}$-espace vectoriel) ; ce module est appelé la représentation régulière de A. Notre définition initiale de kG n'est qu'un cas particulier de ça.

Nous allons pouvoir calculer $\mathrm{End}_G(kG)$. Notons en général $\mathrm{End}_A(V)$ pour les endomorphismes du A-module V, de sorte que $\mathrm{End}_{kG}(V) = \mathrm{End}_G(V)$ pour les G-modules. Alors il est très simple de déterminer $\mathrm{End}_A(A)$, en toute généralité. En effet soit $f\colon A \longrightarrow A$ un homomorphisme de A-modules, et soit $a = f(1)$. Alors $f(x) = f(x\cdot 1) = xf(1) = xa$, et en particulier on peut reconstruire f à partir de a. Il en résulte une application injective $\theta\colon \mathrm{End}_A(A) \longrightarrow A$. Elle est aussi surjective car si on part de $a \in A$, alors $f\colon x \mapsto xa$ appartient bien à $\mathrm{End}_A(A)$ et $\theta(f) = a$.

Attention cependant, θ n'est pas (tout-à-fait) un homomorphisme d'anneaux : vérifiez, on a $\theta(fg) = \theta(g)\theta(f)$. On dira que c'est un anti-isomorphisme, ou encore un isomorphisme $\mathrm{End}_A(A) \longrightarrow A^{op}$, où A^{op} est l'algèbre A avec la multiplication « opposée ».

Revenons au cas $A = kG$, et découvrons que $\mathrm{End}_G(kG) = \mathrm{End}_{kG}(kG) = kG^{op}$. On peut en tirer deux conclusions. Tout d'abord, si kG est semi-simple (par exemple si $k = \mathbf{C}$), alors le (3) de la proposition 1.2.2 affirme que $\mathrm{End}_G(kG)$ est un produit d'algèbres de matrices. Une remarque simple est que $M_n(K)^{op}$ est isomorphe à $M_n(K)$, par l'application $A \mapsto {}^tA$ (la transposée), puisque ${}^t(AB) = {}^tB\,{}^tA$. Donc $kG = \mathrm{End}_G(kG)^{op}$ est encore un produit d'algèbres de matrices. Normalement vous avez déjà vu ce résultat.

Notre deuxième conclusion est que dans le cas où G est un p-groupe (non-trivial) et k est de caractéristique p, alors on a une deuxième bonne raison d'affirmer que kG n'est pas semi-simple. En effet, il suffit de montrer que kG n'est pas isomorphe à un produit d'algèbres de matrices. Pour ceci, on prend $g \neq 1$ dans G, dont l'ordre est p^r, et on calcule

$$(g-1)^{p^r} = g^{p^r} - 1 = 0\,.$$

(On est en caractéristique p !) Les éléments $g-1$ avec $g \neq 1$ engendrent un sous-espace N de codimension 1 dans kG, et on peut montrer (cf exercice 6) que tous les éléments de N sont nilpotents. En fait tout élément de kG s'écrit $x = \alpha 1 - n$ avec $\alpha \in k$, $1 =$ l'élément neutre de G, et $n \in N$; si $\alpha = 0$ alors x est nilpotent, et si $\alpha \neq 0$ alors x est inversible, d'inverse $\frac{1}{\alpha}(1 + \frac{n}{\alpha} + \frac{n^2}{\alpha^2} + \frac{n^3}{\alpha^3} + \cdots)$. Or dans une algèbre de matrices de dimension > 1, il existe des éléments qui ne sont ni inversibles, ni nilpotents (prendre une matrice ayant 0 comme valeur propre, mais ayant une autre valeur propre non-nulle). Pour que kG soit un produit d'algèbres de matrices, il faudrait qu'elle soient toutes de dimension 1, donc toutes des corps ; mais alors il n'y aura pas d'éléments nilpotents non-nuls, et c'est une contradiction.

Terminons en listant quelques propriétés plus « attendues » des modules semi-simples. En fait dans le cas $k = \mathbf{C}$ où tous les modules sont semi-simples, on n'a pas du tout à se poser ce genre de questions.

Proposition 1.2.4. *1. Soit U un module semi-simple, et soit V un sous-module. Alors il existe un sous-module W de U tel que $U = V \oplus W$.*

2. Tout quotient d'un module semi-simple est semi-simple.

3. Tout sous-module d'un module semi-simple est semi-simple.

Démonstration. Pour le (1) écrivons $U = S_1 \oplus \cdots S_n$ avec S_i simple, et utilisons la notation $S_I = \oplus_{i \in I} S_i$ pour chaque partie $I \subset \{1, \ldots n\}$. Choisissons alors I maximal parmi les parties vérifiant $S_I \cap V = 0$, et montrons que $U = S_I \oplus V$ (la somme étant évidemment directe).

Si ce n'était pas le cas, on trouverait j tel que S_j n'est pas inclus dans $S_I + V$, donc $S_j \cap (S_I + V) = 0$ par simplicité de S_j. Mais alors $I \cup \{j\}$ pourrait remplacer I, ce qui contredit la maximalité de I. On a donc bien le (1) avec $W = S_I$.

Le (2) est facile : en gardant les mêmes notations, U/V est isomorphe à S_I, qui est bien semi-simple.

Pour le (3), si $V \subset U$ est un sous-module, alors par le (1) on a W tel que $U = V \oplus W$, donc $V \cong U/W$, et le (2) montre que V est semi-simple. □

§3. Modules indécomposables

On dira qu'un G-module U est *indécomposable* si l'on ne peut pas écrire $U = V \oplus W$ avec $V \neq 0$ et $W \neq 0$. Lorsque $k = \mathbf{C}$, ou plus généralement lorsque tous les modules sont semi-simples, alors les modules indécomposables sont exactement les modules simples, il n'y a pas de différence. Le cas général est bien plus riche.

Voici un critère utile pour reconnaître les modules indécomposables. On dira qu'un anneau A est *local* si chaque $a \in A$ est soit inversible, soit nilpotent. Par exemple un corps est local, dans ce sens.

Proposition 1.3.1. *Soit U un G-module. Si l'anneau $\mathrm{End}_G(U)$ est local, alors U est indécomposable.*

Si on suppose que k est algébriquement clos, alors la réciproque est vraie.

Démonstration. Si $U = V \oplus W$, alors on peut définir $f : U \longrightarrow U$ qui est égal à l'identité sur V, et à 0 sur W. Alors f n'est ni inversible, ni nilpotent. La contraposée de ce que nous venons de montrer affirme que si $\mathrm{End}_G(U)$ a la propriété annoncée, alors U est indécomposable.

Montrons la réciproque, en supposant k algébriquement clos. Pour toute application linéaire $f \in \mathrm{End}(U)$, on peut toujours écrire

$$U = \bigoplus_{\lambda \in k} E_\lambda$$

où E_λ est « l'espace propre généralisé », c'est-à-dire l'espace des $v \in U$ tels que $(f - \lambda Id)^n v = 0$ pour au moins un entier n. (On factorise le polynôme caractéristique, puis théorème des noyaux.) Si on suppose de plus que $f \in \mathrm{End}_G(U)$, alors chaque E_λ est un sous-G-module.

Lorsque U est indécomposable, on doit avoir $E_\lambda = 0$ pour tous les λ sauf un. Si cette unique valeur propre est nulle, alors f est nilpotent ; si elle est non-nulle, alors f est inversible. □

Exemple 1.3.2. Dans l'exemple 1.2.3, nous avons montré que $\mathrm{End}_G(kG)$ avait la propriété ci-dessus (ie, est local) lorsque G est un p-groupe et k est de caractéristique p. On en conclut que la représentation régulière kG est indécomposable dans ce cas. Par contre ça n'est certainement pas un module simple, puisqu'il est non-trivial.

Exemple 1.3.3. Voici encore un exemple qui devrait apparaître frappant, par rapport à la situation sur les complexes. On va écrire C_n pour le groupe cyclique, isomorphe à $\mathbf{Z}/n\mathbf{Z}$, en notation multiplicative ; donc C_n possède un générateur x tel que $C_n = \{1, x, x^2, \ldots, x^{n-1}\}$. Dans l'exercice 2 on donne un exemple de module indécomposable V_n pour $G = C_p \times C_p$ de dimension $2n$ sur k ; on y arrive pour tout k de caractéristique p et tout entier $n \geq 1$.

Comme les modules V_n ont tous des dimensions différentes, on constate avec émoi qu'ils ne sont pas isomorphes les uns aux autres. Le groupe G possède donc une infinité de modules indécomposables différents ! Que l'on compare avec la situation sur $k = \mathbf{C}$, où les indécomposables (qui coïncident avec les irréductibles dans ce cas) sont toujours en nombre fini.

Théorème 1.3.4 (Krull-Schmidt)**.** *Si M est un G-module sur k, où k est algébriquement clos, et si on a deux décompositions*

$$M = U_1 \oplus \cdots \oplus U_r\,,$$

$$M = V_1 \oplus \cdots \oplus V_s\,,$$

où les U_i et les V_i sont indécomposables, alors $r = s$ et après une renumérotation si nécéssaire, on a $U_i \cong V_i$ pour tout i.

On montre d'abord le lemme suivant :

Lemme 1.3.5. *Si A est un anneau local (non supposé commutatif), alors l'ensemble des éléments nilpotents de A est un idéal.*

On vous le laisse en exercice. Pour le théorème, voici une esquisse.

Esquisse. Soit ρ_i la projection sur V_i dont le noyau est la somme des V_j pour $j \neq i$. Soit π la projection sur U_1, dont le noyau est la somme des U_j pour $j \neq 1$. Enfin, soit $p_i = \pi \circ \rho_i$, vu comme endomorphisme de U_1.

Puisque U_1 est indécomposable, $\mathrm{End}(U_1)$ est local, et chaque p_i est soit inversible, soit nilpotent. D'après le lemme, si tous les p_i sont nilpotents, alors leur somme aussi. Or, la somme $p_1 + p_2 + \cdots + p_s$ est l'identité de U_1. Donc il y a un indice i tel que p_i est inversible. Après renumérotation si nécessaire, disons que $p_1 = \pi \circ \rho_1$ est inversible.

On en déduit que ρ_1 et π sont des isomorphismes sans trop de problème. Puisque ρ_1 vaut 0 sur $V_2 + V_3 + \cdots$, on a donc $U_1 \cap (V_2 + V_3 + \cdots) = \{0\}$ et pour des raisons de dimension on a finalement $M = U_1 + V_2 + \cdots + V_s$. On finit par récurrence. □

Corollaire 1.3.6. *On suppose k algébriquement clos. Si on a des modules M, U et V tels que $M \oplus U \cong M \oplus V$, alors $U \cong V$.*

§4. Modules projectifs

On dit qu'un module pour l'algèbre A est *libre* s'il est isomorphe à A^n pour un certain n. Puisque nos G-modules ne sont pas autre chose que des modules pour l'algèbre kG, on peut parler d'un G-module libre, et il s'agit d'un module isomorphe à une somme directe de copies de la « représentation régulière » kG.

Un module P sera dit *projectif* lorsqu'il existe un module V tel que $P \oplus V$ est libre (brièvement, on dit que P est une sommande dans un module libre). Dans le cas $k = \mathbf{C}$, comme vous le savez, tout G-module irréductible est une sommande dans $\mathbf{C}G$ (c'est d'ailleurs une explication possible du fait qu'il n'y a dans ce cas qu'un nombre fini d'irréductibles différents), et par suite, tous les modules sont projectifs. Il est donc normal que le concept n'ait pas été introduit plus tôt. Par contre dans le cours d'algèbre homologique vous avez vu que les modules projectifs étaient au cœur de bien des considérations.

Il y a une définition équivalente de la projectivité : P est projectif si et seulement si, pour tout homomorphisme surjectif $\pi\colon A \longrightarrow B$, et tout homomorphisme $f\colon P \longrightarrow B$, on peut trouver un relèvement $\tilde{f}\colon P \longrightarrow A$ tel que $\pi(\tilde{f}(a)) = f(a)$. Normalement vous connaissez cette équivalence, qui est facile à montrer de toute façon.

Certains modules peuvent être à la fois projectifs et indécomposables, évidemment. Par exemple si on écrit kG comme une somme de modules indécomposables, alors ils sont aussi projectifs. Par ailleurs, le théorème de Krull-Schmidt (valable lorsque $k = \overline{k}$) a pour conséquence que tout module projectif indécomposable est isomorphe à une sommande de kG (on verra un autre argument ci-dessous). Dans le cas où G est un p-groupe et où k est de caractéristique p nous savons que kG est indécomposable (exemple 1.3.2), et donc il n'y a qu'un seul module qui soit à la fois projectif et indécomposable, et c'est kG lui-même – qui est libre ! Cette remarque est suffisamment importante pour être mise en valeur :

Proposition 1.4.1. *Lorsque k est de caractéristique p, et que G est un p-groupe, les modules projectifs sont tous libres.*

Démonstration. On se convainc rapidement que l'énoncé est équivalent à dire qu'il n'y a qu'un seul module à la fois projectif et indécomposable, et que ce module est kG lui-même. Nous avons donc montré la proposition dans la discussion ci-dessus dans le cas où $k = \overline{k}$.

Mais le cas général est facile à déduire. Si $P \oplus U = kG$ avec $P \neq 0$, alors en étendant les scalaires à $\overline{k}$, c'est-à-dire en appliquant $- \otimes_k \overline{k}$, on obtient $\overline{P} \oplus \overline{U} = \overline{k}G$, avec $\overline{P} = P \otimes \overline{k}$ et $\overline{U} = U \otimes \overline{k}$. On en déduit $\overline{U} = 0$ par le cas précédent, et donc $U = 0$. □

Notre premier objectif est de montrer qu'il y a une bijection entre les modules qui sont à la fois projectifs et indécomposables, d'une part, et les modules simples d'autre part. Pour cela, nous aurons besoin de définir le *radical* d'un module. Tout d'abord, un sous-module M d'un module V est dit maximal lorsqu'il n'existe aucun module N tel que $M \subset N \subset V$, à part bien sûr $N = M$ et $N = V$. Il revient exactement au même de dire que V/M est un module simple. On définit alors $\mathrm{rad}(V)$, pour tout module V, comme étant l'intersection des sous-modules maximaux de V.

Lemme 1.4.2. *Le sous-module* $\mathrm{rad}(V)$ *est caractérisé comme étant le plus petit sous-module* U *de* V *tel que le quotient* V/U *est semi-simple.*

Démonstration. Soit $M_1, \dots, M_r$ des sous-modules maximaux de V tels que $\mathrm{rad}(V) = \cap M_i$. Alors $V/\mathrm{rad}(V)$ s'injecte dans $V/M_1 \oplus \cdots \oplus V/M_r$, c'est donc un module semi-simple en vertu de la proposition 1.2.4.

Il faut montrer que c'est le plus petit sous-module avec cette propriété, donc que si on a un module U tel que $V/U = S_1 \oplus \cdots S_s$ avec S_i simple, alors $\mathrm{rad}(V) \subset U$. Or si on nomme $\pi\colon V \to V/U$ la projection, et si $U_i = \pi^{-1}(\oplus_{j\neq i} S_j)$, alors $V/U_i \cong S_i$ et U_i est maximal ; de plus U est l'intersection des U_i, clairement. Comme $\mathrm{rad}(V)$ est l'intersection de *tous* les sous-modules maximaux, il est inclus dans U. □

Corollaire 1.4.3. *Soit* $f\colon V \longrightarrow W$ *un homomorphisme. Alors* $f(\mathrm{rad}(V)) \subset \mathrm{rad}(W)$.

Démonstration. Soit $U = f^{-1}(\mathrm{rad}(W))$. Il suffit de montrer que $\mathrm{rad}(V) \subset U$, et d'après le lemme ça sera automatiquement le cas si on peut montrer que V/U est semi-simple. Or V/U s'injecte dans $W/\mathrm{rad}(W)$. □

Théorème 1.4.4. *On suppose que* k *est algébriquement clos.*

Lorsque P *est un module projectif indécomposable, le module* $P/\mathrm{rad}(P)$ *est simple. Tout module simple peut s'obtenir de cette façon. Si* $P/\mathrm{rad}(P)$ *est isomorphe à* $Q/\mathrm{rad}(Q)$*, où* P *et* Q *sont tous les deux projectifs indécomposables, alors* P *et* Q *sont isomorphes.*

En d'autres termes, on obtient par $P \mapsto P/\mathrm{rad}(P)$ *une bijection entre les modules projectifs indécomposables (à isomorphisme près) et les modules simples (à isomorphisme près).*

Démonstration. Soit P projectif et indécomposable. Pour tout $f \in \mathrm{End}_G(P)$, on a $f(\mathrm{rad}(P)) \subset \mathrm{rad}(P)$ par le dernier corollaire, et on a donc une application induite $\overline{f}\colon P/\mathrm{rad}(P) \longrightarrow P/\mathrm{rad}(P)$. Tout ceci nous donne un homomorphisme d'anneaux $\phi\colon \mathrm{End}_G(P) \longrightarrow \mathrm{End}_G(P/\mathrm{rad}(P))$.

Montrons que ϕ est surjectif. Si on part d'un endomorphisme $g\colon P/\mathrm{rad}(P) \to P/\mathrm{rad}(P)$, on considère la composition $f = g \circ \pi\colon P \to P/\mathrm{rad}(P) \to P/\mathrm{rad}(P)$, où on a appelé π l'application quotient $P \to P/\mathrm{rad}(P)$. Puisque P est projectif, on peut trouver $\tilde{f}\colon P \to P$ tel que $\pi \circ \tilde{f} = f$. Ceci signifie précisément que $\phi(\tilde{f}) = g$. Voir le diagramme ci-dessous.

$$\begin{array}{ccc} P & \xrightarrow{\tilde{f}} & P \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ P/\mathrm{rad}(P) & \xrightarrow{g} & P/\mathrm{rad}(P) \end{array}$$

Le module P étant indécomposable, tout élément de l'anneau $\mathrm{End}_G(P)$ est soit inversible, soit nilpotent, par la proposition 1.3.1. Il en est donc de même pour l'anneau $\mathrm{End}_G(P/\operatorname{rad}(P))$, qui est l'image par ϕ du précédent, et la même proposition nous dit que $P/\operatorname{rad}(P)$ est indécomposable, en plus d'être semi-simple. C'est donc que $P/\operatorname{rad}(P)$ est simple.

Soit V un module quelconque, et soit $v \in V$. Le G-module engendré par v est l'espace vectoriel engendré par les gv pour $g \in G$, mais c'est aussi l'ensemble des av pour $a \in kG$; on a un homomorphisme de modules $kG \longrightarrow V$ qui envoie a sur av. Si on suppose que V est simple, alors l'image de cet homomorphisme, qui est non-nul dès que l'on prend $v \neq 0$, doit être V tout entier.

Maintenant prenons une décomposition du module libre kG en sommandes P_1, …, P_r indécomposables : ces sommandes sont des modules projectifs. Notre homomorphisme $kG = \oplus P_i \longrightarrow V$ ne peut pas être nul sur tous les P_i, donc il y en a un, que nous appellerons P, tel que V est un quotient de P. Les quotients semi-simples de P sont des quotients de $P/\operatorname{rad}(P)$, mais $P/\operatorname{rad}(P)$ et V étant tous les deux simples, ils doivent être isomorphes. Ceci montre la deuxième partie.

Enfin, supposons que $g\colon P/\operatorname{rad}(P) \longrightarrow Q/\operatorname{rad}(Q)$ est un isomorphisme. On peut trouver f comme dans le diagramme commutatif suivant, puisque P est supposé projectif :

$$\begin{array}{ccc} P & \xrightarrow{f} & Q \\ \downarrow & & \downarrow \\ P/\operatorname{rad}(P) & \xrightarrow{g} & Q/\operatorname{rad}(Q) \end{array}$$

On ne peut certainement pas avoir $f(P) \subset \operatorname{rad}(Q)$ (sinon la composition avec $Q \to Q/\operatorname{rad}(Q)$ serait 0, ce qui contredit le diagramme). Or $Q/\operatorname{rad}(Q)$ est simple, nous l'avons vu, ce qui signifie que $\operatorname{rad}(Q)$ est maximal, mais c'est aussi l'intersection de *tous* les sous-modules maximaux. On en conclut que c'est *le seul* sous-module maximal, et que $f(P)$ n'est contenu dans *aucun* sous-module maximal. Donc $f(P) = Q$. Puisque Q est projectif, on en déduit que $Q \oplus U \cong P$ pour un certain U, mais alors $U = 0$ puisque P est indécomposable. Ainsi, P et Q sont isomorphes. □

Remarque. Au cours de la démonstration, on a vu que tout module simple était en fait de la forme $P/\operatorname{rad}(P)$ *avec P une sommande de kG*. Ceci redémontre, étant donnée la bijection du théorème, que tout module à la fois projectif et indécomposable est une sommande dans kG.

Dans le cas d'un p-groupe, la situation est très claire (et nous n'apprenons rien de nouveau, en fait) : il n'y a qu'un seul module simple, c'est le module trivial ; et effectivement, il n'y a qu'un seul module projectif indécomposable, et c'est kG.

Exercices

Exercice 1. On considère un corps k algébriquement clos, et $G = \mathbf{Z}$ (groupe cyclique infini !). Décrire les G-modules simples et les G-modules indécomposables (de dimension finie sur k).

Indication : Jordan. Ça sera le seul exemple de groupe G infini que nous allons regarder.

Exercice 2. Soit $G = C_p \times C_p$, et soit k un corps de caractéristique p. On note x et y pour deux générateurs de G (de sorte que G est l'ensemble des $x^a y^b$ pour $a, b \in \mathbf{Z}/p\mathbf{Z}$).

Soit V_n l'espace vectoriel k^{2n}, dont la base canonique sera notée $v_1, \ldots, v_n, w_1, \ldots, w_n$. Soit $X : V_n \longrightarrow V_n$ l'application linéaire telle que $Xw_i = 0$ et $Xv_i = w_i$, pour tout i. Soit également $Y : V_n \longrightarrow V_n$ l'application linéaire telle que $Yw_i = 0$ pour tout i, alors que $Yv_i = w_{i+1}$ pour $1 \leq i < n$, et enfin $Yv_n = 0$.

1. Vérifier que $X^2 = Y^2 = 0$ et que $XY = YX (= 0)$. Puis, montrer qu'on peut faire de V_n un G-module en exigeant $x \cdot v = (I + X)v$ et $y \cdot v = (I + Y)v$ pour tout $v \in V_n$.
2. Écrire les matrices correspondantes $\rho(x)$ et $\rho(y)$.
3. Montrer qu'une matrice commute avec $\rho(x)$ et $\rho(y)$ si et seulement si elle est de la forme
$$\begin{pmatrix} A & 0 \\ C & A \end{pmatrix}$$
avec $AN = NA$, où
$$N = \begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ \vdots & \ddots & \ddots & \\ 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Puis, en déduire que A est de la forme

$$A = \begin{pmatrix} \lambda_1 & & & & \\ \lambda_2 & \lambda_1 & & & \\ \lambda_3 & \lambda_2 & \lambda_1 & & \\ \vdots & & & \ddots & \\ \lambda_n & & & & \lambda_1 \end{pmatrix}.$$

4. Montrer que l'algèbre $\mathrm{End}_G(V_n)$ est locale, et conclure que V_n est indécomposable.

Exercice 3. On va étudier les modules d'un groupe cyclique.

1. (a) Soit k un corps algébriquement clos, et soit G un groupe abélien. Montrer que les modules simples de G sont de dimension 1.

   (b) On suppose jusqu'à la fin que k est de caractéristique p, que $n = p^a e$ où p ne divise pas e, et que $G = C_n$ est cyclique d'ordre n. Décrire les modules simples de G. Il y en a e différents.

2. (a) Soit T un endomorphisme d'un espace vectoriel V sur k de dimension finie. On suppose que T ne possède qu'une seule valeur propre λ, et que $T^n = I$. Montrer que $(T - \lambda I)^{p^a} = 0$.
   Indication : vérifier que $\lambda^e = 1$; par conséquent le polynôme $X - \lambda$ divise $X^e - 1$.

   (b) A l'aide de Jordan et de la question précédente, décrire tous les modules indécomposables de G. Il y en a n.

3. (a) Faire l'exercice 4.

   (b) En déduire la description des modules projectifs et indécomposables de G.

4. Décrire le radical de chaque module indécomposable.
   Indication : par récurrence sur la taille du bloc de Jordan. Il n'y a qu'un seul module maximal non-trivial dans chaque module indécomposable.

Exercice 4.

1. Soit H un sous-groupe de G. Montrer que kG est libre comme kH-module.
2. En déduire que si P est un kG-module projectif, alors il est aussi projectif comme kH-module. (*Dans la suite du cours nous noterons P_H pour le module P considéré comme kH-module.*)
3. On suppose que l'ordre de G est $n = p^a e$ où p ne divise pas e, et que k est de caractéristique p. Montrer que la dimension d'un module projectif pour G est divisible par p^a.

Exercice 5. Finir la démonstration du lemme 1.3.5 et du théorème 1.3.4.

Exercice 6. Un idéal (bilatère) N d'une algèbre A est dit *nilpotent* s'il existe un entier n tel que $x_1 x_2 \cdots x_n = 0$ si les $x_i \in N$. Dans cet exercice, on va montrer que si G est un groupe d'ordre p^r, si $A = kG$ où k est un corps de caractéristique p, et si N est l'idéal « d'augmentation », c'est-à-dire $N = \{\sum \alpha_g\, g \in kG \mid \sum \alpha_g = 0\}$, alors N est nilpotent.

Préliminaires : vérifier que N est engendré (comme espace vectoriel) par les éléments $g - 1$ pour $g \in G$. Puis, montrer le résultat sur N en utilisant librement les résultats de ce chapitre.

Notre but est cependant de donner une démonstration élémentaire et directe, afin de donner du sens à l'exemple 1.2.3 (deuxième partie).

1. Montrer le résultat dans le cas où G est abélien.
2. Soit H un sous-groupe distingué de G, et soit I un idéal nilpotent de kH. Soit J l'idéal engendré dans kG par I. Montrer que J est également nilpotent.
3. Soit $G' = [G, G]$ le « groupe dérivé » (engendré par les commutateurs $g^{-1}h^{-1}gh$) ; soit I son idéal d'augmentation et J comme ci-dessus. Enfin, soient $g, h \in G$ et $x = g - 1$, $y = h - 1$. Vérifier que $xy - yx \in J$.
4. Montrer qu'il existe un entier n tel que si $x_i \in N$, alors $x_1 x_2 \cdots x_n \in J$.
5. Conclure par récurrence. (*Il est nécessaire de savoir que si G est un p-groupe alors G' est strictement plus petit que G.*)

Chapitre 2

Les théorèmes de Carlson et Chouinard

On suppose que k est un corps algébriquement clos de caractéristique p.

§1. Représentations induites

Lorsque H est un sous-groupe de G, et que M est un H-module, alors on peut définir un G-module noté $M^{\uparrow G}$ et appelé le module induit par M. Pour ceux qui connaissent (bien) les produits tensoriels (même sur un anneau non-commutatif), on peut donner la définition suivante :

$$M^{\uparrow G} = kG \otimes_{kH} M\,.$$

Sinon, de manière plus élémentaire, on peut commencer par le produit tensoriel sur k, c'est-à-dire $kG \otimes_k M$, considérer le sous-espace vectoriel U engendré par les éléments de la forme $h \otimes m - 1 \otimes hm$ (pour $h \in H$, $m \in M$), et alors

$$M^{\uparrow G} = (kG \otimes_k M)/U\,,$$

que l'on voit comme un G-module par $g \cdot \sigma \otimes m = g\sigma \otimes m$.

De manière encore plus simple, si N est un G-module, alors $N \cong M^{\uparrow G}$ si et seulement si ce qui est décrit dans le reste de ce paragraphe est vrai. Le module N possède un sous-espace vectoriel, disons V, qui est stable par l'action de H et qui est isomorphe à M comme H-module. Pour chaque $g \in G$, l'espace $g \cdot V$ est inchangé si on remplace g par gh avec $h \in H$, donc on peut noter σV pour $\sigma \in G/H$. Alors N est la somme directe des σV, où σ parcourt G/H.

Ce critère ne montre pas que $M^{\uparrow G}$ existe, mais il donne une description concrète une fois qu'on est convaincu de l'existence.

§2. Le théorème de Carlson

C'est peut-être le théorème le plus important du cours. Son énoncé fait intervenir les *p-groupes élémentaires abéliens*, c'est-à-dire les groupes de la forme C_p^r pour un certain r.

Théorème 2.2.1 (Carlson)**.** *Il existe un entier τ, qui ne dépend que de G, et des sous-groupes élémentaire abéliens E_1, E_2, …, E_τ de G, avec la propriété suivante. Si U est un G-module, alors il existe un module V tel que la somme directe $U \oplus V$ possède une filtration*

$$\{0\} = L_0 \subset L_1 \subset \cdots \subset L_\tau = U \oplus V$$

où chaque L_i est un G-module, de sorte que $L_i/L_{i-1} \cong W_i^{\uparrow G}$ pour un certain E_i-module W_i.

Nous ne démontrerons pas ce théorème. La preuve est assez longue, mais pas foncièrement difficile, et fait appel à de l'algèbre homologique (sans toutefois entrer dans les finesses de la cohomologie des groupes).

Dans ce chapitre nous allons montrer comment on se réduit au cas où $U = k$ et G est un p-groupe, cas que nous ne traiterons pas. Ensuite nous montrerons le théorème de Chouinard comme conséquence. Les résultats du chapitre suivant seront aussi des applications du théorème de Carlson.

Il est intéressant de se demander quel serait le pendant du théorème en caractéristique 0 (ou en caractéristique qui ne divise pas l'ordre du groupe, en général). Nous avons vu que tout module dans ce cas est projectif, donc sommande dans $(kG)^n$; or le module kG est induit. En effet, il suffit de prendre le sous-groupe trivial $H = \{1\}$ et le module trivial k, et alors $k^{\uparrow G} \cong kG$.

L'énoncé du théorème de Carlson est alors vrai avec $\tau = 1$ et $E_1 = \{1\}$: tout module est une sommande d'un module induit depuis le groupe trivial (qui est élémentaire abélien, pour tout p !). Dans le cas général, en caractéristique p, il faut prendre en compte d'autres sous-groupes élémentaires abéliens. C'est donc encore un exemple d'un phénomène qui passe inaperçu en caractéristique 0.

§3. Réciprocité de Frobenius

(Les résultats de ce paragraphe sont valables sans restriction sur le corps k.)

Lorsque H est un sous-groupe de G, il existe aussi une opération très simple de *restriction*, qui à un G-module M associe M_H, le même espace vectoriel avec l'action de H seulement. La loi de réciprocité de Frobenius exprime une relation très utile entre restriction et induction.

Proposition 2.3.1 (Réciprocité de Frobenius)**.** *Il y a un isomorphisme de G-modules*

$$M \otimes N^{\uparrow G} \cong (M_H \otimes N)^{\uparrow G},$$

pour tout G-module M et tout H-module N.

Notons que l'énoncé fait appel aux produits tensoriels de G-modules : on se souviendra que l'action de G sur $U \otimes V$ est donnée par $g \cdot (u \otimes v) = gu \otimes gv$.

Démonstration. Choisissons des représentants $\sigma_0 = 1, \sigma_1, \ldots, \sigma_k$ pour les classes à gauche de H, de sorte que les éléments de G/H sont précisément H, $\sigma_1 H, \ldots, \sigma_k H$. Comme on l'a vu, pour tout H-module U, les éléments de $U^{\uparrow G}$ peuvent s'écrire $\sum_i \sigma_i \cdot u_i$ avec $u_i \in U$, de manière unique.

Il est donc licite de définir un homomorphisme

$$M \otimes N^{\uparrow G} \longrightarrow (M_H \otimes N)^{\uparrow G}$$

par la règle $m \otimes \sigma_i \cdot n_i \mapsto \sigma_i \cdot (\sigma_i^{-1} m \otimes n)$. On définit également

$$(M_H \otimes N)^{\uparrow G} \longrightarrow M \otimes N^{\uparrow G}$$

par $\sigma_i \cdot (m \otimes n) \mapsto \sigma_i m \otimes \sigma_i n$. On vérifie sans difficulté que ces deux homomorphismes sont inverses l'un de l'autre, et sont compatibles avec l'action de G. □

Nous pouvons tout de suite appliquer ceci pour réduire la démonstration du théorème de Carlson au cas $U = k$:

Proposition 2.3.2. *Si le théorème de Carlson est vrai pour $U = k$, alors il est vrai pour n'importe quel G-module U.*

Démonstration. Supposons donc que $k \oplus V$ ait une filtration $L_O \subset L_1 \subset \cdots$ telle que L_i/L_{i-1} sont isomorphe au module induit $W_i^{\uparrow G}$. Tensorisons tout avec U : nous voyons que $U \otimes (k \oplus V) = U \oplus U \otimes V$ est filtré par les modules $U \otimes L_i$. On a

$$(U \otimes L_i)/(U \otimes L_{i-1}) \cong U \otimes (L_i/L_{i-1})$$

(« exactitude à droite de $U \otimes -$ »), et

$$U \otimes (L_i/L_{i-1}) \cong U \otimes W_i^{\uparrow G} \cong (U_{E_i} \otimes W_i)^{\uparrow G}$$

par la réciprocité de Frobenius. Donc le théorème est vrai pour U. □

Écartons-nous juste un moment du théorème de Carlson pour indiquer des conséquences remarquables de la réciprocité de Frobenius. Pour commencer,

rappelons que si M et N sont deux G-modules, alors $\mathrm{Hom}(M,N)$, l'espace des homomorphismes entre M et N, est aussi un G-module, avec l'action

$$(g\cdot f)(m) = gf(g^{-1}m)\,.$$

En particulier le dual $M^* = \mathrm{Hom}(M,k)$ est un G-module. De plus on a un isomorphisme de G-modules

$$M^*\otimes N \longrightarrow \mathrm{Hom}(M,N)$$

en voyant le tenseur $f\otimes n$ comme l'application $M\to N$ qui envoie m sur $f(m)n$. (Pour se convaincre que c'est un isomorphisme, on prend des bases pour M et N, puis la base duale correspondante pour M^*, et on se rend compte que l'on est en train de vérifier que tout élément de $\mathrm{Hom}(M,N)$ est donné par une unique matrice dans ces bases.)

Avec cette remarque simple et la réciprocité de Frobenius appliquée à M^* et N, on déduit :

Lemme 2.3.3. *Il y a un isomorphisme de G-modules*

$$\mathrm{Hom}(M_H,N)^{\uparrow G}\cong \mathrm{Hom}(M,N^{\uparrow G})\,.$$

Nous aurons besoin de parler des vecteurs fixés par G dans le module M, donc les $m\in M$ tels que $g\cdot m = m$ pour tout $g\in G$. Ils forment un sous-module qui est parfois noté M^G mais c'est trop proche de notre notation pour les modules induits ; nous écrirons $\mathrm{H}^0(G,M)$ pour le module des vecteurs fixés par G, pour des raisons que vous devriez connaître.

Lemme 2.3.4. *Soit M un H-module, où H est un sous-groupe de G. Il y a un isomorphisme (d'espaces vectoriels) entre $\mathrm{H}^0(H,M)$ et $\mathrm{H}^0(G,M^{\uparrow G})$.*

Démonstration. Les σ_i sont comme dans une démonstration précédente. Si $m\in M$ est fixé par H, le vecteur $\sum_i \sigma_i\cdot m\in M^{\uparrow G}$ est fixé par G.

Réciproquement, si $v=\sum_i\sigma_i\cdot m_i$ est fixé par G, alors en particulier comme il est fixé par H on a $m_0\in \mathrm{H}^0(H,M)$; par ailleurs en examinant l'équation $\sigma_i\cdot v = v$ on déduit que $m_i = m_0$.

On en déduit que $m\mapsto \sum_i\sigma_i\cdot m$ est un isomorphisme de $\mathrm{H}^0(H,M)$ sur $\mathrm{H}^0(G,M^{\uparrow G})$. □

Nous pouvons finalement combiner ces petits résultats à l'aide de la remarque suivante : si $f\in\mathrm{Hom}(M,N)$ est fixé par G, cela signifie précisément que c'est un homomorphisme de G-modules. En symboles

$$\mathrm{H}^0(G,\mathrm{Hom}(M,N)) = \mathrm{Hom}_G(M,N)\,.$$

On en déduit :

Lemme 2.3.5. *Il y a un isomorphisme (d'espaces vectoriels) entre* $\mathrm{Hom}_H(M_H, N)$ *et* $\mathrm{Hom}_G(M, N^{\uparrow G})$.

Démonstration. L'espace $\mathrm{Hom}_G(M, N^{\uparrow G})$ est constitué des vecteurs fixés par G dans $\mathrm{Hom}(M, N^{\uparrow G})$, et ce module est isomorphe à $\mathrm{Hom}(M_H, N)^{\uparrow G}$, qui est induit depuis H. D'après le dernier lemme, l'espace des vecteurs fixés par G est isomorphe à celui des vecteurs fixés par H dans $\mathrm{Hom}(M_H, N)$, c'est-à-dire $\mathrm{Hom}_H(M_H, N)$. □

On a utilisé le lemme 2.3.4 pour montrer le lemme 2.3.5, mais on peut aussi faire le contraire : si on sait que le lemme 2.3.5 est vrai, alors on peut prendre $M = k$, le module trivial, et dans ce cas $\mathrm{Hom}_H(M_H, N) = \mathrm{Hom}_H(k_H, N) = \mathrm{H}^0(H, N)$, alors que $\mathrm{Hom}_G(M, N^{\uparrow G}) = \mathrm{Hom}_G(k, N^{\uparrow G}) = \mathrm{H}^0(G, N^{\uparrow G})$.

§4. G-ensembles

Lorsque X est un G-ensemble, c'est-à-dire un ensemble (toujours supposé fini, pour nous) avec une action (à gauche) de G, on peut former le G-module kX ou $k[X]$: c'est exactement analogue à la construction de kG que nous avons donnée. Les vecteurs de kX sont de la forme $\sum_{x\in X} \alpha_x\, x$ avec $\alpha_x \in k$, et l'action de G prolonge celle donnée sur X.

La raison qui nous pousse à parler des G-ensembles maintenant est l'observation suivante : soit k_H le module trivial k, vu comme H-module ; alors $k_H^{\uparrow G} = k[G/H]$. (En particulier kG est obtenu en induisant le module trivial du sous-groupe trivial $H = \{1\}$.) Voilà qui améliore un peu notre intuition vis-à-vis des modules induits. De plus le lemme suivant va pouvoir s'appliquer.

Lemme 2.4.1. *Si* $|X|$ *est premier à* p *(la caractéristique de* k*), alors il existe un module* V *tel que* $kX = k \oplus V$.

Démonstration. On définit $\psi\colon kX \to k$ par $\psi(x) = 1$ pour tous les $x \in X$, et on définit $\phi\colon k \to kX$ par

$$\phi(\alpha) = \frac{\alpha}{|X|} \sum_{x\in X} x\,,$$

ce qui a un sens puisque $|X|$ est inversible dans k. La composition $\psi \circ \phi$ est l'identité, donc si on pose $\pi = \phi \circ \psi$ on a $\pi^2 = \pi$. Le module $V = \ker(\pi)$ convient alors. □

Comme promis, nous pouvons montrer :

Proposition 2.4.2. *Si le théorème de Carlson est vrai pour tous les* p*-groupes, alors il est vrai pour tous les groupes.*

Démonstration. Soit G un groupe quelconque, on veut montrer que le théorème de Carlson est vrai pour $U = k$, ce qui est suffisant d'après la dernière proposition. Soit P un p-groupe de Sylow de G, de sorte que $X = G/P$ est d'ordre premier à p. D'après le lemme il existe V_1 tel que $kX = k_P^{\uparrow G} = k \oplus V_1$. Il suffit donc de montrer qu'il existe V_2 tel que $k_P^{\uparrow G} \oplus V_2 = k \oplus V_1 \oplus V_2$ possède une filtration comme annoncée. En d'autre termes, on veut montrer le théorème de Carlson dans le cas $U = k_P^{\uparrow G}$.

Pour ceci, on applique le théorème à P, puisqu'on le suppose vrai pour les p-groupes. Il existe donc un P-module M tel que $k_P \oplus M$ soit filtré par des modules L_i comme dans le théorème, c'est-à-dire avec $L_i/L_{i-1} \cong W_i^{\uparrow P}$. Maintenant on « induit tout jusqu'à G ». On conclut que $k_P^{\uparrow G} \oplus M^{\uparrow G}$ est filtré par des modules $L_i^{\uparrow G}$ (il faut se convaincre que si $N_1 \subset N_2$ alors $N_1^{\uparrow G} \subset N_2^{\uparrow G}$, ce qui est facile).

Pour conclure, deux petites propriétés des modules induits à observer. Tout d'abord, comme le processus d'induction est un produit tensoriel, on a bien

$$L_i^{\uparrow G}/L_{i-1}^{\uparrow G} \cong (L_i/L_{i-1})^{\uparrow G} = (W_i^{\uparrow P})^{\uparrow G}\,.$$

Ensuite, l'induction est transitive : on a $(W_i^{\uparrow P})^{\uparrow G} = W_i^{\uparrow G}$, comme le vérifie tout de suite. □

§5. Le théorème de Chouinard

C'est le suivant :

Théorème 2.5.1 (Chouinard)**.** *Soit M un G-module. Alors M est projectif si et seulement si le module M_E est projectif pour chaque sous-groupe élémentaire abélien $E \subset G$.*

Notons que M_E est projectif si et seulement s'il est libre, puisque E est un p-groupe.

On va montrer le théorème dans le reste de ce paragraphe. Commençons par signaler qu'une « moitié » du théorème est très facile. En effet nous avons vu à l'occasion d'un exercice que le module $(kG)_E$ est libre, pour tout sous-groupe E ; par suite, si M est projectif, c'est-à-dire une sommande dans $(kG)^n$, alors M_E est une sommande dans le module libre $(kG)_E^n$, donc il est projectif (et ceci pour tout sous-groupe).

Passons à l'implication difficile, et supposons que M_E est projectif, comme kE-module, pour tout sous-groupe élémentaire abélien E. Appliquons le théorème de Carlson, pour trouver V tel que $k \oplus V$ est filtré par les L_i, comme d'habitude. De nouveau, tensorisons tout par M, de sorte que $M \oplus M \otimes V$ est filtré par les modules $M \otimes L_i$. On peut écrire, et ce n'est pas la première fois, que

$$(M \otimes L_i)/(M \otimes L_{i-1}) \cong M \otimes W_i^{\uparrow G} \cong (M_{E_i} \otimes W_i)^{\uparrow G}\,.$$

Soit $E = E_i$ pour un certain i, et $W = W_i$. Montrons d'abord que $M_E \otimes W$ est libre. On sait que M_E est libre car il est projectif et que E est un p-groupe, disons $M_E \cong kE^n$. Or $kE = k^{\uparrow G}$, le module trivial k du sous-groupe trivial $\{1\}$ induit jusqu'à E. Donc $kE \cong (k^n)^{\uparrow G}$ et

$$M_E \otimes W \cong (k^n \otimes W_{\{1\}})^{\uparrow E}$$

par réciprocité de Frobenius. Bien sûr $k^n \otimes W_{\{1\}}$ est trivial (le groupe étant trivial !), donc en l'induisant à E on obtient un somme directe de copies de kE, c'est-à-dire un module libre.

On sait donc que $M_E \otimes W \cong (kE)^m = (k^m)^{\uparrow E}$ pour un certain m. Par transitivité de l'induction $(M_E \otimes W)^{\uparrow G} = (k^m)^{\uparrow G} = (kG)^m$. Le module $(M_E \otimes W)^{\uparrow G}$ est donc libre.

La fin de la démonstration est donnée par le lemme suivant, dont on vous confie la démonstration :

Lemme 2.5.2. *Soit U un module filtré par des sous-modules*

$$U_0 = \{0\} \subset U_1 \subset U_2 \subset \cdots \subset U_r = U\,.$$

On suppose que U_{i+1}/U_i est libre. Alors U est lui-même libre.

Exercices

Exercice 7. Montrer le lemme 2.5.2.

Exercice 8. On prend $G = C_9 = \{1, x, x^2, \ldots, x^8\}$ le groupe cyclique d'ordre 9, et k un corps de caractéristique 3. Soit $X = x - 1 \in kG$, de sorte que $kG = k[X]/(X^9)$. Enfin, soit $V = kG/(X^8)$.

On considère le module $k \oplus V$ et ses éléments $a = (1, 0)$ et $b = (0, 1)$. Soit L_1 le sous-module engendré par $a + X^5 b$ et L_2 le sous-module engendré par a et $X^3 b$.

Montrer que L_1, L_2/L_1 et $(k \oplus V)/L_2$ sont tous isomorphes à $k_H^{\uparrow G}$ où $H = \langle x^3 \rangle$ est le sous-groupe d'ordre 3 dans G.

Indication : le module $k_H^{\uparrow G}$ est l'unique module dans lequel l'action de x est donnée par un bloc de Jordan de taille 3 de valeur propre 1.

Chapitre 3

Les théorèmes de Quillen

Saur précision contraire, k est algébriquement clos, de caractéristique p.

§1. Cohomologie

Nous allons avoir besoin de parler de l'espace vectoriel noté

$$\mathrm{Ext}^n_{kG}(M,N) \quad \text{ou} \quad \mathrm{Ext}^n_G(M,N)\,,$$

lorsque M et N sont des G-modules. Rappelons que pour $n=0$ on a

$$\mathrm{Ext}^0_G(M,N) = \mathrm{Hom}_G(M,N)\,.$$

Si l'on fixe N, on peut affirmer que $M \mapsto \mathrm{Ext}^n_G(M,N)$ est le n-ième foncteur dérivé à droite du foncteur $M \mapsto \mathrm{Hom}_G(M,N)$. En particulier en présence d'une suite exacte courte

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

on obtient une suite exacte longue

$$\cdots \to \mathrm{Ext}^n_G(C,N) \to \mathrm{Ext}^n_G(B,N) \to \mathrm{Ext}^n_G(A,N) \to \mathrm{Ext}^{n+1}_G(C,N) \to \cdots$$

Mais il est également vrai que, M étant fixé, le foncteur $N \mapsto \mathrm{Ext}^n_G(M,N)$ est le n-ième foncteur dérivé à droite de $N \mapsto \mathrm{Hom}_G(M,N)$. Une suite exacte courte comme ci-dessus donne naissance à une suite exacte longue

$$\cdots \to \mathrm{Ext}^n_G(M,A) \to \mathrm{Ext}^n_G(M,B) \to \mathrm{Ext}^n_G(M,C) \to \mathrm{Ext}^{n+1}_G(M,A) \to \cdots$$

Rappelons enfin que si M est projectif, ou si N est « injectif », alors pour $n>0$ on a $\mathrm{Ext}^n_G(M,N)=0$. (Il y a une définition générale de ce qu'est

un module injectif, que vous avez vue dans le cours de cohomologie, et que nous ne répèterons pas ici ; cependant, pour les modules sur kG, les modules injectifs sont les mêmes que les modules projectifs, comme on le verra dans l'exercice 9).

Une propriété basique est l'additivité, ie $\mathrm{Ext}^n_G(M, N\oplus N') = \mathrm{Ext}^n_G(M,N)\oplus \mathrm{Ext}^n_G(M,N')$ et $\mathrm{Ext}^n_G(M\oplus M', N) = \mathrm{Ext}^n_G(M,N)\oplus \mathrm{Ext}^n_G(M',N)$. Bien plus profond, l'existence de produits : si $x \in \mathrm{Ext}^n_G(M,N)$ et $y \in \mathrm{Ext}^m_G(N,L)$, on peut former leur produit, qui appartient à $\mathrm{Ext}^{n+m}_G(M,L)$, et que l'on va noter xy ou $x\cdot y$. ATTENTION, dans de nombreuses sources vous verrez cet élément noté yx au lieu de xy (très certainement à cause de la notation $y\circ x$ dans le cas $n=m=0$). Notre convention va simplifier *énormément* certains énoncés dans le chapitre suivant.

En particulier $\mathrm{Ext}^n_G(M,M)$ est un anneau, dont l'unité est $Id \in \mathrm{Hom}_G(M,M) = \mathrm{Ext}^0_G(M,M)$. En général il n'est ni commutatif, ni gradué-commutatif.

Lorsque $M = k$, on note

$$\mathrm{H}^n(G,N) = \mathrm{Ext}^n_G(k,N)\,.$$

On parle du n-ième *groupe de cohomologie de G à coefficients dans N* (en fait c'est plus qu'un groupe, c'est un espace vectoriel sur k). Notez alors que pour $n=0$ on a

$$\mathrm{H}^0(G,N) = \mathrm{Hom}_G(k,N) = \text{ les points fixes dans } N\,.$$

Lorsque $N = k$, on obtient l'anneau de cohomologie $\mathrm{H}^*(G,k)$. Il est gradué-commutatif (donc commutatif lorsque k est de caractéristique 2).

Exemple 3.1.1. On va donner quelques exemples de calcul. On va utiliser le fait, qui est une conséquence du « théorème des coefficients universels », que

$$\mathrm{H}^*(G,k) \cong \mathrm{H}^*(G,\mathbf{F}_p)\otimes_{\mathbf{F}_p} k$$

pour tout corps k de caractéristique p. En pratique les calculs sont toujours faits avec $\mathbf{F}_p$.

Soit $G = C_2$, le groupe à 2 éléments, et soit k un corps de caractéristique 2. Alors

$$\mathrm{H}^*(G,k) = k[x]\,,$$

où x est de degré 1. D'après la formule de Künneth, on a donc

$$\mathrm{H}^*(C_2^r,k) = k[x_1,\ldots,x_r]$$

où chaque x_i est de degré 1.

Pour $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, le groupe des quaternions d'ordre 8, on a

$$\mathrm{H}^*(G,k) = k[x,y,z]/(x^3, x^2+xy+y^2)\,,$$

avec x et y de degré 1 et z de degré 4. (Les relations entrainent $y^3 = 0$ et sont en fait symmétriques en x et y.)

Pour $G = D_8$, le groupe diédral d'ordre 8, on a

$$\mathrm{H}^*(G,k) = k[x,y,z]/(xy)\,,$$

avec x et y de degré 1 et z de degré 4.

Soit maintenant p un nombre premier impair, et soit k un corps de caractéristique p. Alors

$$\mathrm{H}^*(C_p,k) = k[x,u]/(u^2)\,,$$

avec x de degré 2 et u de degré 1 ; c'est donc une algèbre commutative. Par Künneth on a

$$\mathrm{H}^*(C_p^r,k) = k\langle x_1,\dots,x_r,u_1,\dots,u_r\rangle/(u_i^2, u_iu_i + u_ju_i)\,.$$

Ce n'est pas une algèbre commutative puisque $u_iu_j = -u_ju_i$, mais elle est bien graduée-commutative. (C'est le produit tensoriel d'une algèbre de polynômes et d'une algèbre « extérieure », comme vous avez dû en rencontrer en cours de calcul différentiel.)

Lorsque $H \subset G$ est un sous-groupe, on a un homomorphisme d'anneaux, dit « de restriction »

$$\mathrm{res}_{G,H}\colon \mathrm{H}^*(G,k) \longrightarrow \mathrm{H}^*(H,k)\,.$$

On peut montrer que dans ce cas $\mathrm{H}^*(H,k)$ est finiment engendré comme $\mathrm{H}^*(G,k)$-module.

En fait plus généralement, un homomorphisme de groupes $f\colon H \to G$ induit un homomorphisme d'anneaux $f^*\colon \mathrm{H}^*(G,k) \to \mathrm{H}^*(H,k)$. Il y a un cas particulier qu'il faut connaître : lorsque $G = H$ et $f(x) = g^{-1}xg$ pour un $g \in G$, alors f^* est l'identité.

§2. Le lemme d'Eckmann-Shapiro

Proposition 3.2.1 (Eckmann-Shapiro)**.** *Il existe un isomorphisme d'espaces vectoriels*

$$\mathrm{Ext}^n_G(M, N^{\uparrow G}) \cong \mathrm{Ext}^n_H(M_H, N)\,,$$

qui de plus est naturel en M et N.

Démonstration. Calculons $\mathrm{Ext}^n_G(M, N^{\uparrow G})$ d'abord. Pour cela nous avons le loisir de choisir une résolution projective quelconque P_* de M par des G-modules. L'homologie du complexe $\mathrm{Hom}_G(P_*, N^{\uparrow G})$ donne les groupes $\mathrm{Ext}^n_G(M, N^{\uparrow G})$.

Les modules $(P_*)_H$ sont projectifs comme H-modules, comme on le sait, et l'opération de restriction à H préservant clairement les suites exactes, on

constate que $(P_*)_H$ est une résolution projective de M_H. Pour calculer le groupe $\mathrm{Ext}^n_H(M_H, N)$, on peut donc prendre le n-ième groupe d'homologie du complexe $\mathrm{Hom}_H((P_*)_H, N)$.

C'est là que nous appliquons le lemme 2.3.5 qui affirme que

$$\mathrm{Hom}_G(P_*, N^{\uparrow G}) \cong \mathrm{Hom}_H((P_*)_H, N)\,.$$

À titre d'exercice, on vous laisse le soin de vérifier que le lemme 2.3.5 que nous venons d'appliquer est « naturel », c'est-à-dire qu'ici l'isomorphisme est compatible avec les différentielles. On calcule donc bien la même chose dans les deux cas, d'où un isomorphisme

$$\mathrm{Ext}^n_G(M, N^{\uparrow G}) \cong \mathrm{Ext}^n_H(M_H, N)$$

comme annoncé. Là encore on vous laisse montrer la naturalité. □

§3. Premier théorème de Quillen

Il y a plusieurs résultats qui mériteraient le nom de « théorème de Quillen » (pas seulement parce que Quillen était un mathématicien prolifique, mais aussi parce que nous allons donner quelques variantes d'un de ses résultats). Le premier que nous allons donner utilise les notations du théorème de Carlson pour k : on a donc un entier τ, des sous-groupes élémentaires abéliens E_i pour $0 \leq i \leq \tau$, et un module V tel que $U = k \oplus V$ a une filtration comme annoncé.

Théorème 3.3.1. *Soient $x_1, x_2, \ldots, x_\tau \in \mathrm{H}^*(G, k)$ des éléments (homogènes) tels que $\mathrm{res}_{G,E_i}(x_i) = 0$. Alors $x_1 x_2 \cdots x_\tau = 0$.*

Démonstration. L'anneau $\mathrm{H}^*(G,k) = \mathrm{Ext}^*_G(k,k)$ est une sommande directe dans $\mathrm{Ext}^*_G(U,U)$. On va considérer x_i comme un élément de $\mathrm{Ext}^*_G(U,U)$ et montrer que le produit des x_i fait 0 dans cet anneau.

On va regarder les suites exactes

$$0 \longrightarrow L_{i-1} \xrightarrow{j_i} L_i \xrightarrow{q_i} W_i^{\uparrow G} \longrightarrow 0\,.$$

On utilise maintenant (sans démonstration, on suppose cela connu) le fait que les suites exactes longues des Exts sont compatibles avec les multiplications, dans le sens où le diagramme suivant est commutatif :

$$\begin{array}{ccccccc}
\cdots \longrightarrow & \mathrm{Ext}^r_G(U, L_{i-1}) & \xrightarrow{(j_i)_*} & \mathrm{Ext}^r_G(U, L_i) & \xrightarrow{(q_i)_*} & \mathrm{Ext}^r_G(U, W_i^{\uparrow G}) & \longrightarrow \\
& \downarrow{\scriptstyle x_i\times} & & \downarrow{\scriptstyle x_i\times} & & (\dagger)\ \downarrow{\scriptstyle x_i\times} & \\
\cdots \longrightarrow & \mathrm{Ext}^{r+m_i}_G(U, L_{i-1}) & \xrightarrow{(j_i)_*} & \mathrm{Ext}^{r+m_i}_G(U, L_i) & \xrightarrow{(q_i)_*} & \mathrm{Ext}^{r+m_i}_G(U, W_i^{\uparrow G}) & \longrightarrow
\end{array}$$

Enfin, par Eckmann-Shapiro on a aussi un diagramme commutatif

$$\begin{array}{ccc} \mathrm{Ext}^r_G(U, W_i^{\uparrow G}) & \xrightarrow{\cong} & \mathrm{Ext}^r_{E_i}(U_{E_i}, W_i) \\ \Big\downarrow{\scriptstyle x_i \times} & & \Big\downarrow{\scriptstyle \mathrm{res}_{G,E_i}(x_i)\times} \\ \mathrm{Ext}^{r+m_i}_G(U, W_i^{\uparrow G}) & \xrightarrow{\cong} & \mathrm{Ext}^{r+m_i}_{E_i}(U_{E_i}, W_i) \end{array}$$

Par hypothèse $\mathrm{res}_{G,E_i}(x_i) = 0$ et on en déduit que l'application marquée (†) dans le diagramme ci-dessus est nulle.

Commençons la démonstration proprement dite par le cas $i = \tau$, donc $L_\tau = U$, et $r = 0$. On peut considérer l'élément $Id_U \in \mathrm{Ext}^0_G(U, U) = \mathrm{Ext}^0_G(U, L_\tau)$, c'est même l'unité de cette algèbre. On vient de voir que $(q_\tau)_*(x_\tau Id_U) = 0$ donc $x_\tau Id_U = x_\tau$ est de la forme $(j_r)_*(\phi_r)$ pour un certain $\phi_r \in \mathrm{Ext}^{m_\tau}_G(U, L_{\tau-1})$ (on écrit m_i pour le degré de x_i).

Supposons maintenant par récurrence que l'on a montré que

$$x_{i+1}x_{i+2}\cdots x_\tau = (j_\tau)_* \circ (j_{\tau-1})_* \circ \cdots \circ (j_{i+1})_*(\phi_{i+1})$$

pour un certain $\phi_{i+1} \in \mathrm{Ext}^r_G(U, L_i)$ (avec r approprié). En multipliant par x_i il vient :

$$\begin{aligned} x_i \cdots x_\tau &= x_i \times (j_\tau)_* \left[(j_{\tau-1})_* \circ \cdots \circ (j_{i+1})_*(\phi_{i+1})\right] \\ &= (j_\tau)_* \left[x_i \times (j_{\tau-1})_* \circ \cdots \circ (j_{i+1})_*(\phi_{i+1})\right] \\ &= (j_\tau)_* \circ (j_{\tau-1})_* \circ \cdots \circ (j_{i+1})_*(x_i\phi_{i+1})\,. \end{aligned}$$

(Première égalité par définition, deuxième par commutativité du diagramme ci-dessus appliquée pour $i = \tau$, et ensuite on obtient la troisième en recommençant avec $i = \tau - 1$, $\tau - 2$, etc.) Avec un raisonnement similaire à celui ci-dessus, on montre que $x_i\phi_{i+1} = (j_i)_*(\phi_i)$ pour un certain ϕ_i. En répétant cette procédure, on en arrive à

$$x_1x_2\cdots x_\tau = (j_\tau)_* \circ (j_{\tau-1})_* \circ \cdots \circ (j_1)_*(\phi_1)$$

avec $\phi_1 \in \mathrm{Ext}^*_G(U, L_0)$. Or $L_0 = \{0\}$ donc le produit vaut 0 et la preuve est terminée. □

Le corollaire suivant est très proche de l'énoncé originel de Quillen.

Corollaire 3.3.2 (Quillen)**.** *Soit k un corps de caractéristique p. Il existe un entier τ ayant la propriété suivante. Choisissons $E_1, \ldots, E_r$ des représentants des classes de conjugaison des sous-groupes élémentaires abéliens maximaux de G. Si $x \in H^*(G, k)$ vérifie $\mathrm{res}_{G,E_i}(x) = 0$ pour tous les i, alors $x^\tau = 0$.*

L'hypothèse sur les E_i, en clair, est que si E est un p-sous-groupe élémentaire abélien maximal de G, alors E est conjugué à un E_i et un seul. Noter que k n'est pas supposé algébriquement clos, ici.

Démonstration. Puisque $\mathrm{H}^*(G,k) = \mathrm{H}^*(G,\mathbf{F}_p)\otimes k$, on peut se contenter de montrer le corollaire pour $k = \overline{\mathbf{F}}_p$; on en déduit qu'il est vrai pour $\mathbf{F}_p$, et ensuite qu'il est vrai pour k quelconque.

Tout d'abord, si $x \in \mathrm{H}^*(G,k)$ vérifie $\mathrm{res}_{G,E}(x) = 0$ pour absolument *tous* les sous-groupes élémentaires, alors on a bien $x^\tau = 0$ d'après le théorème, en prenant $x_1 = \cdots = x_\tau = x$.

Ensuite, si on restreint cette condition aux sous-groupes E élémentaires qui sont *maximaux*, le résultat reste vrai : en effet si $E_0 \subset E$ sont élémentaires, alors la restriction se factorise comme suit :

$$\mathrm{res}_{G,E_0}\colon \mathrm{H}^*(G,k) \xrightarrow{\mathrm{res}_{G,E}} \mathrm{H}^*(E,k) \xrightarrow{\mathrm{res}_{E,E_0}} \mathrm{H}^*(E_0,k)\,.$$

On constate bien que si $\mathrm{res}_{G,E}(x) = 0$ pour tous les E maximaux, alors c'est vrai pour tous les E, et $x^\tau = 0$.

Enfin, supposons que E et E' soient conjugués, disons $E' = g^{-1}Eg$. Considérons alors le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathrm{H}^*(G,k) & \xrightarrow{f^*} & \mathrm{H}^*(G,k) \\ {\scriptstyle \mathrm{res}_{G,E'}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}_{G,E}} \\ \mathrm{H}^*(E',k) & \xrightarrow{f_0^*} & \mathrm{H}^*(E,k)\,. \end{array}$$

Ici f^* et f_0^* sont toutes les deux induites par l'homomorphisme $x \mapsto g^{-1}xg$. Comme on l'a vu plus haut, f^* est l'identité ; quant à f_0^* ce n'est certainement pas l'identité, mais c'est tout de même un isomorphisme. On repère alors immédiatement que si $\mathrm{res}_{G,E}(x) = 0 = \mathrm{res}_{G,E}(f^*(x)) = f_0^*(\mathrm{res}_{G,E'}(x))$, alors $\mathrm{res}_{G,E'}(x) = 0$.

On conclut finalement que si $\mathrm{res}_{G,E_i}(x) = 0$ pour tous les E_i du corollaire, alors $\mathrm{res}_{G,E}(x) = 0$ pour chaque sous-groupe élémentaire E, et donc $x^\tau = 0$. □

Lorsque $p = 2$, on a une sorte de réciproque : si $x \in \mathrm{H}^*(G,k)$ est nilpotent, c'est-à-dire si $x^n = 0$ pour un certain n, alors $\mathrm{res}_{G,E_i}(x) = 0$ pour chaque i, et pour une raison toute bête : l'anneau $\mathrm{H}^*(E_i,k)$ est un anneau de polynômes dans ce cas, et ne possède pas d'élément nilpotent non-nul.

Exemple 3.3.3. Prenons $G = Q_8$, nous avons vu que

$$\mathrm{H}^*(Q_8,\mathbf{F}_2) = \mathbf{F}_2[x,y,z]/(x^3, x^2+xy+y^2)$$

avec x et y de degré 1 et z de degré 4. Le groupe Q_8 ne possède qu'un seul sous-groupe élémentaire, à savoir $\{\pm 1\} \cong C_2$. Le corollaire affirme donc que les éléments dans le noyau de l'application de restriction

$$\mathrm{res}_{G,C_2}\colon \mathrm{H}^*(G,\mathbf{F}_2) \longrightarrow \mathrm{H}^*(C_2,\mathbf{F}_2) = \mathbf{F}_2[u]$$

sont nilpotents. L'élément z n'est pas nilpotent, donc s'envoie sur un élément non-nul, et donc en l'absence de tout autre choix on conclut que $\mathrm{res}_{G,C_2}(z) = u^4$. Les éléments x et y sont nilpotents (en fait $x^3 = y^3 = 0$) donc $\mathrm{res}_{G,C_2}(x) = \mathrm{res}_{G,C_2}(y) = 0$, par la petite réciproque juste mentionnée.

§4. La dimension de Krull

La *dimension de Krull* d'une algèbre commutative A finiment engendrée sur un corps k est le plus grand entier d tel que A contient une algèbre de polynômes $k[x_1, \ldots, x_d]$. (Dans les livres vous trouverez des variantes de cette définition, qui parfois est restreinte aux algèbres intègres.) La dimension de Krull d'une algèbre graduée-commutative ($ba = (-1)^{|a|\,|b|}ab$) est définie de la même façon (on vérifie que les x_i peuvent être supposés homogènes).

Remarquons que si N est un idéal de A dont tous les éléments sont nilpotents, alors A et A/N ont la même dimension (exercice). Dans le cas où A est graduée-commutative, et où k est de caractéristique $\neq 2$, on peut considérer l'idéal $N = A^{impair}$ engendré par les éléments de degré impair ; ces élements sont nilpotents (et donc tous ceux de N aussi) car si a est de degré impair alors $a^2 = -a^2$, d'où $a^2 = 0$. Donc la dimension de A est la même que celle de $\overline{A} = A/A^{impair}$; or $\overline{A}$ est commutative. On peut donc se ramener au cas commutatif si l'on veut.

Comme nous n'allons utiliser cette notion que dans le cas d'algèbres graduées, on peut s'en remettre au lemme suivant :

Lemme 3.4.1. *Soit A^* une algèbre graduée-commutative. Alors la dimension de Krull de A^* est d si et seulement si d est le plus petit entier tel que* $\dim_k A^n = O(n^{d-1})$.

On vous laisse la démonstration en exercice. Les exemples ci-dessous doivent donner des idées.

Exemple 3.4.2. Pour faire la démonstration, il faut en particulier bien comprendre l'exemple de $A = k[x_1, \ldots, x_d]$ où les générateurs ont tous le même degré, disons $|x_i| = s$. Dans ce cas $\dim_k A^n = 0$ si n n'est pas divisible par s, et $\dim_k A^{sn} = \binom{n+d-1}{d-1}$, ce qui est un polynôme en n de degré $d-1$. Donc $\dim_k A^n = O(n^{d-1})$ (c'est-à-dire que $\dim_k A^n/n^{d-1}$ est borné), et d est clairement minimal. La dimension de Krull de A est d, d'après le lemme. (On peut aussi calculer la dimension en raisonnant avec les *degrés de transcendance*, si on connaît déjà.)

La restriction sur les degrés des x_i ne change rien à l'affaire, finalement : montrez-le. En gros, si x_i est de degré a_i, alors on peut prendre un multiple commun s des a_i, disons $s = a_i b_i$, et alors l'algèbre $k[x_1^{b_1}, \ldots, x_d^{b_d}] \subset A^*$ est une algèbre de polynômes avec le même nombre de variables, mais ces variables ont toutes le même degré s.

Exemple 3.4.3. Si maintenant $A = \oplus A_i$ où A_i est un anneau de dimension d_i, le lemme montre immédiatement que la dimension de Krull de A est $\max_i d_i$. Même si chaque A_i est un anneau de polynômes, c'est déjà pénible à montrer directement (sans le lemme).

Exemple 3.4.4. Si $B \subset A$, alors la dimension de B est $\leq$ à celle de A, clairement. Maintenant, si l'on suppose que A est de type fini comme B-module (et que tout est gradué, pour que le lemme s'applique), alors les dimensions sont égales : en effet si A est un quotient de B^m pour un certain m fixé, alors la dimension de A en un degré donné est asympotiquement la même que celle de B.

En géométrie algébrique on montre des résultats similaires sans supposer que les algèbres sont graduées, mais c'est plus dur et nous n'en aurons pas besoin.

Le résultat suivant, très joli, est encore dû à Quillen.

Théorème 3.4.5 (Quillen)**.** *La dimension de Krull de* $\mathrm{H}^*(G, \overline{\mathbf{F}}_p)$ *est le plus grand* d *tel que* G *contient un sous-groupe de la forme* C_p^d*.*

Démonstration. Nous avons déjà remarqué que si N est un idéal de A dont tous les éléments sont nilpotents, alors A/N a la même dimension que A.

Par exemple si K est le noyau de la restriction $\mathrm{H}^*(G, k) \longrightarrow \oplus_i \mathrm{H}^*(E_i, k)$, où la notation est comme dans le corollaire 3.3.2, alors ce même corollaire nous dit que $\mathrm{H}^*(G, k)/K$ a la même dimension que $\mathrm{H}^*(G, k)$.

Pour les même raisons, l'anneau $\mathrm{H}^*(E_i, k)$ a la même dimension que l'anneau de polynômes obtenu en quotientant par l'idéal engendré par les éléments de degré impair (ceci pour p impair ; si $p = 2$ on ne quotiente par rien du tout). Cette dimension est d_i où $E_i \cong C_p^{d_i}$ (cf premier exemple).

D'après les résultats des deux derniers exemples ci-dessus, la dimension de Krull de $\mathrm{H}^*(G, k)$ est bien $\max_i d_i$. □

Exemple 3.4.6. Si on continue l'exemple 3.3.3 avec le groupe Q_8, on constate bel est bien que la dimension de Krull est 1 : en fait l'algèbre graduée $\mathrm{H}^*(G, \mathbf{F}_2)$ est *périodique* de période 4, c'est-à-dire que $\dim A^n = \dim A^{n+4}$, et dans ce cas le calcul de la dimension par le lemme donne bien 1. Par ailleurs le groupe Q_8 possède un sous-groupe C_2 mais pas de sous-groupe de la forme C_2^r avec $r \geq 2$, comme prévu.

Exercices

Exercice 9. On rappelle que M^* désigne le dual du module M, et que tous les modules sont de dimension finie sur k.

1. Montrer que M est projectif si et seulement si M^* est injectif, et *vice versa*.
2. Montrer que kG est isomorphe à $(kG)^*$.
   Indication. Considérer $\varepsilon\colon kG \to k$ *l'homomorphisme défini par* $\varepsilon(\sum \alpha_g g) = \alpha_1$*, puis la forme bilinéaire* $kG \times kG \to k$ *définie par* $x, y \mapsto \langle x, y\rangle = \varepsilon(xy)$*. Montrer que* $\phi\colon kG \to (kG)^*$ *donné par* $\phi(x) = \langle x, -\rangle$ *est l'isomorphisme recherché.*
3. Conclure que M est projectif si et seulement s'il est injectif.

Exercice 10. Montrer le lemme 3.4.1.

Exercice 11. Soit $G = D_8$, le groupe diédral d'ordre 8. Examiner les assertions du corollaire 3.3.2 et du théorème 3.4.5 dans ce cas (dans l'esprit de ce qu'on a fait pour Q_8).

Chapitre 4

Introduction aux variétés algébriques

On va développer un tout petit peu le langage des variétés algébriques, infiniment moins qu'on ne le ferait dans un cours de géométrie algébrique évidemment. Ceci va être pratique pour formuler encore un « théorème de Quillen », et dans le chapitre suivant nous aurons aussi besoin de variétés.

§1. Variétés algébriques

Soit k un corps quelconque (pour l'instant), et A une algèbre sur k, commutative (nous généraliserons un peu ci-dessous) et finiment engendrée. On va noter

$$\mathrm{Spec}(A) = \mathrm{Hom}_{k-\mathrm{alg}}(A, k) = \{\text{homomorphismes de } k-\text{algèbres } A \longrightarrow k\}\,.$$

Pour nous $\mathrm{Spec}(A)$ est simplement un ensemble. Dans d'autres contextes on met beaucoup plus de structure sur cet objet, mais pour nos besoins il sera déjà assez parlant d'examiner les relations entre différents ensembles $\mathrm{Spec}(A)$ pour différentes algèbres A. Au fait, un ensemble de la forme $\mathrm{Spec}(A)$ est appelé une *variété algébrique affine*. (Il y en a des non-affines, mais nous n'en parlerons pas.)

Exemple 4.1.1. Commençons par l'exemple de $A = k[x_1, \ldots, x_n]$. Un homomorphisme $f\colon A \to k$ est alors entièrement spécifié par les valeurs $f(x_i) \in k$. On a donc une bijection

$$\mathrm{Spec}(k[x_1, \ldots, x_n]) \cong k^n\,.$$

Pour l'intuition, on pense vraiment à $\mathrm{Spec}(k[x])$ comme à une droite, à $\mathrm{Spec}(k[x, y])$ comme à un plan, etc.

En général, puisque nous supposons que A est finiment engendrée comme k-algèbre, cela signifie que l'on a un homomorphisme surjectif

$$\phi\colon k[x_1,\dots,x_n] \longrightarrow A$$

et donc une identification $A \cong k[x_1,\dots,x_n]/I$ où $I = \ker(\phi)$. L'anneau $k[x_1,\dots,x_n]$ étant nœthérien, on peut trouver des polynômes $P_1,\dots,P_r$ (en nombre fini !) engendrant l'idéal I.

Si on veut alors se donner $f\colon A \to k$, il faut spécifier des valeurs $f(x_i) \in k$ de façon à ce que $f(P_j(x_1,\dots,x_n)) = 0 = P_j(f(x_1),\dots,f(x_n))$. On a donc une bijection

$$\mathrm{Spec}(A) \cong \{(y_1,\dots,y_n) \in k^n \mid P_j(y_1,\dots,y_n) = 0 \text{ pour chaque } j\}\,.$$

On pense donc à $\mathrm{Spec}(A)$ comme à un sous-ensemble de k^n défini par des équations polynomiales. Par exemple $\mathrm{Spec}(k[x,y]/(x^2+y^2-1))$ est un cercle, informellement.

Une remarque simple : un homomorphisme $\phi\colon B \longrightarrow A$ donne naissance à une application $\phi^*\colon \mathrm{Spec}(A) \longrightarrow \mathrm{Spec}(B)$. Dans l'exemple en cours, c'est l'inclusion de $\mathrm{Spec}(A)$ dans k^n, en prenant $B = k[x_1,\dots,x_n]$.

Bien sûr ϕ n'est pas unique, pas plus que l'entier n ou les polynômes P_j. Mais d'autres choix mènent à un isomorphismes d'anneaux

$$f\colon \frac{k[x_1,\dots,x_n]}{I} \longrightarrow \frac{k[t_1,\dots,t_m]}{J}\,.$$

On a donc une bijection

$$f^*\colon \mathrm{Spec}\left(\frac{k[t_1,\dots,t_m]}{J}\right) \longrightarrow \mathrm{Spec}\left(\frac{k[x_1,\dots,x_n]}{I}\right)\,.$$

Si on pense à f^* comme à une application d'une partie de k^m vers une partie de k^n, alors en inspectant les définitions on constate qu'elle est donnée par des équations polynomiales, c'est-à-dire $f(t_1,\dots,t_m) = (p_1(t_i),\dots,p_n(t_i))$ où $p_j(t_i)$ est un polynôme en $t_1,\dots,t_m$. Bien sûr il en va de même pour l'inverse de f.

Il y a donc bien des choses qui ne dépendent pas du choix de ϕ. Par exemple, imaginons que $k = \mathbf{R}$ ou $\mathbf{C}$, alors $\mathrm{Spec}(A)$ hérite d'une topologie comme sous-ensemble de k^n, et même d'une structure de variété différentiable avec un peu de chance ; et l'on voit clairement que cette topologie, ou cette structure différentiable, sont préservées si l'on choisit une autre « présentation » que ϕ (puisque la bijection f^* par des équations polynomiales ci-dessus est clairement continue, et même différentiable autant qu'on veut).

Ces concepts sont poussés beaucoup plus loin lorsque l'on fait de la « vraie » géométrie algébrique.

Revenons aux définitions générales. Puisque k est un corps, si $a \in A$ est nilpotent alors $f(a) = 0$ pour tout $f \in \mathrm{Spec}(A)$. Donc $\mathrm{Spec}(A) = \mathrm{Spec}(A/N)$ lorsque N est un idéal ne comprenant que des éléments nilpotents.

À partir de cette remarque simple, on peut étendre la définition de $\mathrm{Spec}(A)$ au cas où A est graduée-commutative au lieu de commutative (alors qu'en général, la non-commutativité va mettre à bas tous les théorèmes de géométrie algébrique, et nous en citerons quelques-uns). En effet si A est une telle algèbre, et si la caractéristique de k est différente de 2, tout homomorphisme de k-algèbres $A \to k$ se factorise par $\overline{A} = A/A^{impair}$ comme précédeùmment, et rappelons que $\overline{A}$ est une algèbre commutative. Ainsi $\mathrm{Spec}(A) = \mathrm{Spec}(\overline{A})$, et tous les théorèmes réservés aux algèbres commutatives vont en fait s'appliquer à $\mathrm{Spec}(A)$. Il n'y a donc pas de danger à traiter $\mathrm{Spec}(A)$ pour ces algèbres comme si de rien n'était.

Si la caractéristique de k est 2, c'est encore plus simple : une algèbre graduée-commutative est en fait commutative dans ce cas.

§2. Encore un théorème de Quillen

Voici un théorème de géométrie algébrique, que nous ne prouverons pas.

Proposition 4.2.1. *On suppose que k est algébriquement clos. Soit $\phi\colon A \longrightarrow B$ un homomorphisme injectif entre k-algèbres (commutatives et finiment engendrées), de sorte que B soit également finiment engendré comme A-module. Alors l'application*

$$\phi^*\colon \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$$

est surjective, et ses fibres sont finies.

(Rappelons que les « fibres » de ϕ^* sont les ensembles $(\phi^*)^{-1}(x)$ pour $x \in \mathrm{Spec}(A)$.) Dans ce cas on pense à $\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ comme à ce qu'on appelle un « revêtement » en topologie.

Pour se donner une idée de la raison pour laquelle k doit être algébriquement clos, et pour faciliter la recherche d'une démonstration de cette proposition dans un livre, voici quelques commentaires. Soit $f\colon A \to k$ un élément de $\mathrm{Spec}(A)$, et soit $M = \ker(f)$. Alors M est un idéal maximal de A, puisque $A/M \cong k$ est un corps. La réciproque est-elle vraie ?

Si M est un idéal maximal de A, alors $K = A/M$ est un corps, qui contient k, et qui est finiment engendré comme algèbre sur k (tout comme A). Dans cette situation, l'une des variantes du théorème que l'on appelle le *Nullstellensatz* affirme que K est une extension algébrique finie de k. Si k est supposé algébriquement clos, alors $K = k$, et l'idéal M définit l'élément $A \longrightarrow A/M = k$ de $\mathrm{Spec}(A)$.

On a donc une description de $\mathrm{Spec}(A)$ comme étant l'ensemble des idéaux maximaux de A dans ce cas. Sachant cela, vous trouverez l'énoncé de la proposition, en termes d'idéaux, dans un cours d'algèbre commutative.

Fixons $k = \overline{\mathbf{F}}_p$ jusqu'à la fin du chapitre. On va énoncer une version géométrique du théorème de Quillen. Une notation standard pour cela est $V_G := \mathrm{Spec}(\mathrm{H}^*(G,k))$. Notez qu'une inclusion $E \subset G$ donne un homomorphisme $\mathrm{res}_{G,E}\colon \mathrm{H}^*(G,k) \to \mathrm{H}^*(E,k)$ et donc finalement une application $V_E \to V_G$.

Théorème 4.2.2. *Soient $E_1, \ldots, E_r$ des représentants des classes de conjugaison des sous-groupes élémentaires abéliens maximaux de G. Alors il existe une application surjective*

$$\coprod V_{E_i} \longrightarrow V_G$$

dont les fibres sont finies.

Lorsque E est élémentaire abélien, l'anneau $\mathrm{H}^*(E,k)$ est un anneau de polynômes (à des éléments nilpotents près qui ne changent pas le Spec), et V_E est un « espace affine » (droite, plan ou autre selon la dimension). Le théorème affirme donc que V_G est essentiellement une union d'espaces affines, « à un revêtement près ».

Démonstration. Soit $K_i = \ker(\mathrm{res}_{G,E_i})$. Si $f\colon \mathrm{H}^*(G,k) \to k$ est un élément de V_G, alors le corollaire 3.3.2 nous dit que f se factorise par $\mathrm{H}^*(G,k)/\cap_i K_i$, puisque les éléments dans l'intersection des K_i sont nilpotents et ne sauraient prendre une autre valeur par f que 0. On a donc $V_G = \mathrm{Spec}(\mathrm{H}^*(G,k)/\cap K_i)$.

Considérons alors l'inclusion

$$\frac{\mathrm{H}^*(G,k)}{\cap_i K_i} \hookrightarrow \bigoplus_i \mathrm{H}^*(G,k)/K_i \hookrightarrow \bigoplus_i \mathrm{H}^*(E_i,k).$$

La dernière proposition s'applique (vérifiez-le). Le théorème en découle directement, en remarquant que $\mathrm{Spec}(A \oplus B) = \mathrm{Spec}(A) \coprod \mathrm{Spec}(B)$. □

§3. Sous-variétés

Soit A une k-algèbre, commutative et de type fini. Si I est un idéal de A, alors on peut définir un certain sous-ensemble de $\mathrm{Spec}(A)$ appelé *sous-variété définie par I*. La définition la plus rapide consiste à remarquer que la projection $\pi\colon A \to A/I$ induit une application $\pi^*\colon \mathrm{Spec}(A/I) \to \mathrm{Spec}(A)$, et par ailleurs en se référant aux définitions on constate immédiatement que π^* est injective ; donc $\mathrm{Spec}(A/I)$ peut être vu comme un sous-ensemble de $\mathrm{Spec}(A)$, et c'est ce sous-ensemble que l'on appelle la variété définie par I (on ne lui attribue pas de notation particulière, à part $\mathrm{Spec}(A/I)$).

Dans le cas idiot où $I = A$, l'algèbre A/I n'ayant qu'un seul élément $0 = 1$, on prend comme convention que $\mathrm{Spec}(A/I)$ est l'ensemble vide, ce qui est cohérent avec la description suivante.

Pour se forger un tout petit peu l'intuition, revenons au cas où $A \cong k[x_1, \ldots, x_n]/J$ où l'idéal J est engendré par les polynômes $P_1, P_2, \ldots P_r$.

On a vu que $\mathrm{Spec}(A)$ s'identifie avec le sous-ensemble de k^n où les polynômes P_i prennent tous la valeur 0. Si $f \in k[x_1, \ldots, x_n]$, on peut voir f comme une fonction sur k^n, et donc sur $\mathrm{Spec}(A)$, à valeurs dans k. Les éléments $f \in J$ induisent la fonction nulle sur $\mathrm{Spec}(A)$, donc finalement on peut même voir les éléments de $k[x_1, \ldots, x_n]/J \cong A$ comme des fonctions sur la variété $\mathrm{Spec}(A)$. *Les éléments de l'algèbre A peuvent être vus comme des fonctions sur* $\mathrm{Spec}(A)$.

En prenant des générateurs $f_1, \ldots, f_s$ de I, on voit $\mathrm{Spec}(A/I)$ comme le sous-ensemble de $\mathrm{Spec}(A)$ sur lequel les f_i s'annulent tous. (Noter que chaque variété algébrique, du coup, est une sous-variété d'un « espace affine » $\mathrm{Spec}(k[x_1, \ldots, x_n])$ pour un certain n.)

Exemple 4.3.1. Soit $A = k[x, y]/(x^2+y^2-1)$. On a vu qu'on pouvait penser à $\mathrm{Spec}(A)$ comme à l'ensemble des couples $(u, v) \in k^2$ vérifiant $u^2 + v^2 = 1$, c'est-à-dire un cercle lorsque $k = \mathbf{R}$. Soit maintenant I l'idéal de A engendré par $x - y$. Alors $\mathrm{Spec}(A/I) = \mathrm{Spec}(k[x, y]/(x^2 + y^2 - 1, x - y))$ est le sous-ensemble du cercle $\mathrm{Spec}(A)$ sur lequel la fonction $x-y$ s'annule ; il comprend les éléments (u, v) vérifiant $u = v$ et $2u^2 = 1$.

Si la caractéristique de k est $\neq 2$, il y a donc deux points de la forme (r, r), où r est l'une des deux racines de $\frac{1}{2}$. Si la caractéristique est 2, on obtient l'équation $0 = 1$, et $\mathrm{Spec}(A/I)$ est l'ensemble vide.

On peut se poser la question réciproque. Soit $f \in A$, auquel on pense comme à une fonction sur $\mathrm{Spec}(A)$. Supposons que f ne prenne que la valeur 0 sur $\mathrm{Spec}(A/I)$. Est-ce que $f \in I$? La réponse est non, mais presque, et c'est le contenu d'un théorème qui s'appelle (encore !) le *Nullstellensatz* qui affirme que dans cette situation, et sous réserve que k soit algébriquement clos, il existe un entier n tel que $f^n \in I$. Notons d'ailleurs que si on ajoute à I tous les éléments f tels que $f^n \in I$ pour un certain n, on obtient un idéal J appelé le *radical* de I, et $\mathrm{Spec}(A/J) = \mathrm{Spec}(A/I)$; donc il était clair que la réponse à notre question devait se faire « au radical près ».

Nous avons donc deux théorèmes qui s'appellent tous les deux le Nullstellensatz (« théorème des zéros »), et en fait ils sont assez proches. Voir les exercices.

On va avoir besoin du cas particulier où A est une algèbre graduée, et où I peut être engendré par des éléments f_i *homogènes*. En écrivant A comme quotient d'une algèbre de polynômes *gradués* $k[x_1, \ldots, x_n]$, chaque f_i s'écrit alors comme une somme de monômes $x_1^{a_1} \cdots x_n^{a_n}$ avec $a_1|x_1| + \cdots + a_n|x_n| = c_i =$ constante. Le cas où l'un des nombres c_i vaut 0 est sans intérêt, puisqu'alors f_i est inversible et $A = I$, de sorte que $\mathrm{Spec}(A/I)$ est vide. Excluant ce cas, on voit qu'aucun f_i n'a de terme constant, et en particulier $\{0\} \in \mathrm{Spec}(A/I)$.

Supposons de plus que A est engendrée par des éléments ayant tous le même degré d. Alors on peut prendre $|x_i| = d$ ci-dessus, et chaque f_i est

composé de monômes vérifiant $\sum_i a_i$ = constante (donc f_i est un « polynôme homogène » au sens élémentaire, comme par exemple une forme quadratique $x_1x_2 + 4x_1^2 - 5x_2^2$). Dans ce cas, on peut dire que $\mathrm{Spec}(A/I)$ est un *cône* dans k^n, dans le sens où pour chaque point $x \in \mathrm{Spec}(A/I)$, toute la droite $\{\lambda x \mid \lambda \in k\}$ est incluse dans $\mathrm{Spec}(A/I)$.

Exemple 4.3.2. Un exemple aussi important que simple est celui où $A = k[x]$. Cet anneau est principal, donc tout idéal est de la forme $I = (P)$. Dans ce cas $\mathrm{Spec}(A/I)$ est un ensemble fini, celui des racines de P dans k.

Dans le cas gradué, un tel ensemble fini ne saurait être un cône que lorsqu'on est dans l'un des cas suivant :

- $\mathrm{Spec}(A/I) = k = \mathrm{Spec}(A)$, ce qui arrive précisément lorsque $P = 0$;
- $\mathrm{Spec}(A/I) = \{0\}$, ce qui arrive précisément lorsque $P = x^k$ pour un certain k ;
- $\mathrm{Spec}(A/I) = \emptyset$, lorsque P est une constante non-nulle.

Exercice

Exercice 12. Lire les deux premiers chapitres de [Bum98]. Le premier théorème que nous avons appelé Nullstellensatz est la proposition 2.3, et le deuxième est le théorème 1.2.

Faire un maximum d'exercices parmi ceux proposés à la fin des chapitres.

Chapitre 5

Variétés-supports

k est un corps algébriquement clos de caractéristique p.

§1. Structures multiplicatives, suite

Rappelons que l'on dispose d'un produit sur les « Exts », qui associe une classe $x \in \mathrm{Ext}^n_G(M,N)$ avec une classe $y \in \mathrm{Ext}^m_G(N,L)$ pour former $xy \in \mathrm{Ext}^{n+m}_G(M,L)$:

$$\mathrm{Ext}^n_G(M,N) \otimes \mathrm{Ext}^m_G(N,L) \longrightarrow \mathrm{Ext}^{n+m}_G(M,L)\,. \qquad (*)$$

En particulier, $\mathrm{Ext}^*(M,N)$ est un module sur l'algèbre $\mathrm{Ext}^*_G(M,M)$, et c'est aussi un module (à droite) sur l'algèbre $\mathrm{Ext}^*_G(N,N)$ (et les deux actions commutent). Mais nous avons surtout besoin de savoir que $\mathrm{Ext}^*(M,N)$ est un module sur $\mathrm{H}^*(G,k)$. Pour ceci, on commence par :

Lemme 5.1.1. *Pour tous G-modules M, N on a un isomorphisme naturel pour chaque $n \geq 0$:*

$$\mathrm{Ext}^n_G(M,N) \cong \mathrm{H}^n(G, M^* \otimes N) = \mathrm{H}^n(G, \mathrm{Hom}(M,N))\,.$$

Démonstration. On l'a vu pour $n = 0$ (voir remarque juste avant le lemme 2.3.5). On vous laisse généraliser en tout degré, comme dans la démonstration de la proposition 3.2.1. □

On a donc deux idées qui nous viennent, et il est important de savoir qu'elles mènent à la même solution. Tout d'abord on note que $\mathrm{Ext}^*_G(k,L) = \mathrm{H}^*(G,L)$ est un module sur l'algèbre $\mathrm{Ext}^*_G(k,k) = \mathrm{H}^*(G,k)$, pout tout L ; donc avec $L = \mathrm{Hom}(M,N)$ et en vertu du lemme, on voit bien que $\mathrm{Ext}^*_G(M,N)$ est un module sur $\mathrm{H}^*(G,k)$ comme on le voulait.

Mais on peut aussi penser à regarder l'homomorphisme d'anneaux $k \to \mathrm{Hom}(M,M)$, qui donne un autre homomorphisme d'anneaux $H^*(G,k) \to H^*(G,\mathrm{Hom}(M,M)) \cong \mathrm{Ext}^*(M,M)$. Puisque $\mathrm{Ext}^*_G(M,N)$ est un module sur $\mathrm{Ext}^*_G(M,M)$, en particulier c'est aussi un module sur $\mathrm{H}^*(G,k)$, par restriction.

Ces deux procédés coïncident. Essayons simplement de reformuler ceci de façon à pouvoir citer un résultat facilement consultable. Il existe un produit « externe »

$$\mathrm{H}^*(G,L) \otimes \mathrm{H}^*(G,L') \longrightarrow \mathrm{H}^*(G, L \otimes L')\,.$$

Si de plus on a une application $L \otimes L' \to L''$, alors il y a une opération

$$\mathrm{H}^*(G,L) \otimes \mathrm{H}^*(G,L') \longrightarrow \mathrm{H}^*(G,L'')\,. \qquad (**)$$

Le résultat « de cohérence » est alors : si $L = \mathrm{Hom}(M,N)$, $L' = \mathrm{Hom}(N,L)$ et $L'' = \mathrm{Hom}(M,L)$, alors (**) est la même chose que (*), *via* l'identification du lemme. Voir la proposition 4.3.8 dans [CTVEZ03].

(Comme cas particulier, l'isomorphisme $\mathrm{Ext}^*_G(M,M) \cong \mathrm{H}^*(G,\mathrm{Hom}(M,M))$ est en fait un isomorphisme *d'anneaux*; nous l'avions sous-entendu ci-desus.)

Ayant ça en tête, on regarde le diagramme commutatif suivant (on rappelle que $\mathrm{End}(M) = \mathrm{Hom}(M,M)$) :

$$\begin{array}{ccccc}
\mathrm{H}^*(G,k) \otimes \mathrm{H}^*(G,\mathrm{Hom}(M,N)) & \longrightarrow & \mathrm{H}^*(G, k \otimes \mathrm{Hom}(M,N)) & \longrightarrow & \mathrm{H}^*(G,\mathrm{Hom}(\\
\downarrow & & \downarrow & & \downarrow \\
(G,\mathrm{End}(M)) \otimes \mathrm{H}^*(G,\mathrm{Hom}(M,N)) & \longrightarrow & \mathrm{H}^*(G, \mathrm{End}(M) \otimes \mathrm{Hom}(M,N)) & \longrightarrow & \mathrm{H}^*(G,\mathrm{Hom}(\
\end{array}$$

Le carré de gauche commute par naturalité de (**), en utilisant l'application $k \to \mathrm{End}(M)$ déjà évoquée; celui de droite est obtenu en appliquant $\mathrm{H}^*(G,-)$ à un carré qui est déjà commutatif. La flèche verticale la plus à droite est l'identité. Les deux chemins entre le coin supérieur gauche et le coin inférieur droit du diagramme, en suivant les bords extérieurs, sont les deux structures de module sur $\mathrm{Ext}^*_G(M,N)$, qui sont donc les mêmes.

Voici ce qu'il faut retenir de la discussion :

Lemme 5.1.2. *$\mathrm{Ext}^*_G(M,N)$ est un module sur $\mathrm{H}^*(G,k)$. De plus, si l'action de $x \in \mathrm{H}^*(G,k)$ est nulle sur $\mathrm{Ext}^*_G(M,M)$ pour un certain module M, alors elle est nulle sur $\mathrm{Ext}^*_G(M,N)$ pour tout module N.*

On va admettre le résultat suivant. On rappelle que tous les G-modules, pour nous, sont de dimension finie sur k.

Théorème 5.1.3 (Evens-Venkov)**.** *Le module $\mathrm{Ext}^*_G(M,N)$ est de type fini sur $\mathrm{H}^*(G,k)$.*

§2. Variétés-supports

On en vient à la définition des variétés-supports. Soit M un G-module, et voyons l'algèbre $\mathrm{Ext}^*_G(M,M)$ comme un module sur l'anneau $\mathrm{H}^*(G,k)$. Soit alors $J(M)$ l'annihilateur de ce module : en clair, c'est l'idéal dans $\mathrm{H}^*(G,k)$ des x tels que $xy=0$ pour tout $y \in \mathrm{Ext}^*(M,M)$. Cet idéal est gradué.

Rappelons que V_G désigne la variété $\mathrm{Spec}(\mathrm{H}^*(G,k))$. On va maintenant écrire $V_G(M)$ pour la sous-variété définie par l'idéal $J(M)$. (Par exemple, vérifiez que $V_G(k)=V_G$.) On l'appelle la *variété-support* de M.

On peut exprimer un bon nombre des propriétés des modules en termes de leurs variétés-supports. Par exemple, on peut montrer que $V_G(M\otimes N) = V_G(M)\cap V_G(N)$, ou encore que si $V_G(M)$ s'écrit comme la réunion de deux sous-variétés de V_G, dont l'intersection est $\{0\}$, alors M est décomposable.

Nous allons nous concentrer sur la démonstration de la propriété suivante.

Proposition 5.2.1. *$V_G(M)=\{0\}$ si et seulement si M est projectif.*

On note que la propriété « $V_G(M)=\{0\}$ » revient à dire que $V_G(M)$ est réduit à un point, puisqu'il s'agit d'une sous-variété associée à un idéal gradué.

Pour la démonstration, nous nous servirons du lemme d'algèbre homologique suivant.

Lemme 5.2.2. *Soit M un G-module. On suppose que pour tout module N il existe un entier $n=n(M,N)$ tel que $\mathrm{Ext}^*_G(M,N)=0$ pour $*\geq n$. Alors M est projectif.*

On donne des indications pour montrer ce lemme dans l'exercice 13.

Démonstration de la proposition 5.2.1. Si M est projectif, alors $L=M^*\otimes M$ aussi, de sorte que $\mathrm{H}^*(G,L)=0$ pour $*>0$. Dans ce cas $J(M)=\mathrm{H}^{>0}(G,k)$, et la sous-variété correspondante ne contient que $\{0\}$.

Voyons la réciproque. Supposons que $V_G(M)=\{0\}$. Soient $x_1,\dots,x_n$ des générateurs de $\mathrm{H}^*(G,k)$. Si on voit x_i comme une fonction sur V_G, alors cette fonction s'annule sur tous les points de $V_G(M)$ (c'est-à-dire sur l'unique point qui est $\{0\}$). Par le Nullstellensatz, $x_i^r \in J(M)$ pour un certain r. Par définition, x_i^r agit trivialement sur $\mathrm{Ext}^*(M,M)$, et donc aussi sur $\mathrm{Ext}^*(M,N)$ pour tout module N par le lemme 5.1.2. Par Evens-Venkov $\mathrm{Ext}^*_G(M,N)$ est finiment engendré comme module sur $\mathrm{H}^*(G,k)$; il en découle que $\mathrm{Ext}^n_G(M,N)=0$ pour tous les n suffisamment grands.

Par le dernier lemme, on en conclut que M est projectif. □

§3. Variétés de rang

On se place maintenant dans le cas où E est un p-groupe élémentaire abélien, disons $E=C_p^n=\langle x_1,\dots,x_n\rangle$. Dans ce cas $kE=k[x_1,\dots,x_n]/(x_i^p-$

1). Si on se donne $\alpha = (\alpha_1, \ldots, \alpha_n) \in k^n$, on peut considérer l'élément

$$u_\alpha = 1 + \sum_i \alpha_i (x_i - 1) \in kE\,.$$

Dans ce cas $u_\alpha^p = 1$, et le sous-groupe du groupe multiplicatif $kE^\times$ engendré par u_α est cyclique d'ordre p (pour $\alpha \neq 0$). Nous dirons que c'est un *sous-groupe cyclique décalé* (shifted cyclic subgroup) de E.

Bien sûr $k\langle u_\alpha \rangle \cong kC_p$ est une sous-algèbre de kE, et on peut parler de la restriction $M_{\langle u_\alpha \rangle}$ d'un G-module.

On définit alors la *variété de rang* $V_E^r(M)$ par

$$V_E^r(M) = \{\alpha \in k^n \mid M_{\langle u_\alpha \rangle} \text{ n'est pas libre comme module sur } k\langle u_\alpha \rangle\}\,.$$

(Par convention $0 \in V_E^r(M)$.)

Exemple 5.3.1. Prenons $E = \langle x, y \rangle = C_p^2$. On a un module M de dimension 2 dans lequel x et y agissent respectivement par

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

où $\lambda \in k$ est un paramètre. (On pourrait écrire M_λ au lieu de M ; exercice : si $\lambda \neq \mu$ alors M_λ et M_μ ne sont pas isomorphes.)

Formons donc $u_\alpha = 1 + \alpha_1(x-1) + \alpha_2(y-1)$. Cet élément agit par

$$A = \begin{pmatrix} 1 & \alpha_1 + \lambda\alpha_2 \\ 0 & 1 \end{pmatrix}$$

Le module M est libre comme $k\langle u_\alpha \rangle$-module si et seulement si la forme de Jordan de A est

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Ça sera le cas précisément quand le rang de $A - I$ est 1, clairement, donc lorsque $\alpha_1 + \lambda\alpha_2 \neq 0$. Par suite $V_E^r(M)$ est la droite

$$\{(\alpha_1, \alpha_2) \in k^2 \mid \alpha_1 + \lambda\alpha_2 = 0\}\,.$$

Un très beau théorème, que nous ne montrerons pas, est le suivant :

Théorème 5.3.2. *Pour $p = 2$, on a*

$$V_E^r(M) = V_E(M)$$

(c'est-à-dire que ce sont les mêmes sous-ensembles de k^n).

Pour $p > 2$, l'application

$$V_E(M) \longrightarrow V_E^r(M)$$

qui envoie $(\alpha_1, \ldots, \alpha_n)$ sur $(\alpha_1^p, \ldots, \alpha_n^p)$ est une bijection.

L'intérêt de ce théorème vient du fait que $V_E^r(M)$ est relativement calculable, alors que $V_E(M)$ l'est beaucoup moins ; mais à l'inverse, $V_E(M)$ a de bonnes propriétés « théoriques », comme celle de la proposition 5.2.1. Savoir que les deux sont en fait les mêmes (pour $p = 2$) ou du moins fortement liées (pour p impair) est donc clairement une bonne nouvelle.

En guise d'application, nous pouvons montrer le « lemme de Dade » (en réalité c'est tricher que de le présenter comme conséquence du théorème, car pour démontrer le théorème l'une des premières étapes serait de montrer le lemme de Dade par un argument direct).

Corollaire 5.3.3 (Lemme de Dade)**.** *Un E-module est projectif si et seulement si pour chaque $\alpha \neq 0$ la restriction $M_{\langle u_\alpha \rangle}$ est projective.*

Ici « projectif » peut être remplacé par « libre » puisque E est un p-groupe et $\langle u_\alpha \rangle$ aussi.

Démonstration. Dans les exercices, vous montrerez que kE est libre comme $k\langle u_\alpha \rangle$-module. Donc si M est libre sur kE et que $M \cong (kE)^n$, alors $M_{\langle u_\alpha \rangle}$ est visiblement libre comme $k\langle u_\alpha \rangle$-module.

C'est la réciproque qui fait appel au théorème. En effet si toutes les restrictions en question sont projectives, alors $V_E^r(M) = \{0\}$. Le théorème affirme alors que $V_E(M) = \{0\}$. La proposition 5.2.1 nous dit bien que M est projectif. □

Si maintenant G est un groupe quelconque, nous appellerons sous-groupe cyclique décalé de G un tel « sous-groupe » $\langle u_\alpha \rangle$ pour $E \subset G$, où E est un p-groupe élémentaire abélien. En combinant le corollaire avec le théorème de Chouinard, on a en fait :

Corollaire 5.3.4. *Un G-module est projectif si et seulement si pour chaque $\alpha \neq 0$ la restriction $M_{\langle u_\alpha \rangle}$ est projective.*

(En d'autres termes, le résultat est valable pour G quelconque, pas seulement pour $G = E$ élémentaire abélien.)

Exercices

Exercice 13. On va démontrer le lemme 5.2.2.

1. Soit M comme dans le lemme. Montrer qu'il existe en fait un entier $n = n(M)$, ne dépendant que de M, tel que $\mathrm{Ext}^*_G(M, N) = 0$ pour $* \geq n$ et tout N.
2. Montrer que si $n(M) = 1$, alors M est projectif.
   Indication : on prend une résolution projective (P_*) de M, on pose $K = \ker(P_0 \to M)$ et on utilise la résolution pour calculer $\mathrm{Ext}^*_G(M, K)$. Déduire du fait que $\mathrm{Ext}^1_G(M, K) = 0$ (par hypothèse) que M est une sommande dans P_0 et est donc projectif.
3. Montrer le cas général par récurrence sur $n(M)$.
   Indication : si on prend une suite exacte

$$0 \longrightarrow L \longrightarrow P \longrightarrow M \longrightarrow 0$$

   avec P projectif, on peut montrer $n(L) = n(M) - 1$ si $n(M) \geq 2$. Puis, on n'oublie pas que les modules projectifs sont injectifs.

Exercice 14. Soit $E = \langle x, y, z \rangle \cong C_2^3$, et soient $A, B, C \in k$ des paramètres. On définit un E-module M de dimension 4, dans lequel x, y et z agissent par les matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & C & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ A & 0 & 1 & 0 \\ 0 & B & 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

respectivement. Montrer que

$$V_E^r(M) = \{(\alpha_1, \alpha_2, \alpha_3) \in k^3 \mid (\alpha_1 + Ax a_2)(\alpha_1 + B\alpha_2) + C\alpha_3^2 = 0\}.$$

Exercice 15. (Critère de projectivité, utilisé dans l'exercice suivant.)
Soit G un p-groupe, et soit $\rho = \sum_{g \in G} g \in kG$.

1. Montrer que $k\rho$ est l'unique idéal minimal de kG.
   Indication : un idéal minimal est un module simple...
2. Soit M un G-module, et $\rho \cdot M = \{\rho m \mid m \in M\}$. Soit $a_1, \ldots, a_t$ une base de l'espace vectoriel $\rho \cdot M$, et soit b_i tel que $\rho b_i = a_i$. On définit
   $$\psi \colon kG^t \longrightarrow M$$
   par $\psi(x_1, \ldots, x_t) = \sum x_i b_i$. Montrer que $\ker \psi = \{0\}$, en utilisant la question précédente.
3. En déduire que $M \cong kG^t \oplus M'$ avec $\rho \cdot M' = \{0\}$.
4. Montrer que
   $$\dim \rho \cdot M \leq \frac{1}{|G|} \dim M \,,$$
   avec égalité si et seulement si M est projectif.

Exercice 16. Avec les notations du cours, montrer que kE est libre comme module sur $k\langle u_\alpha \rangle$ (où $\alpha \neq 0$).

Indication : le cas $n = 2$, donc $E = C_p^2 = \langle x, y \rangle$, est représentatif du cas général. On a donc $u_\alpha = 1 + \alpha_1(x-1) + \alpha_2(y-1)$. On utilise l'exercice précédent, et ici $\rho = 1 + u_\alpha + \cdots + u_\alpha^{p-1} = (u_\alpha - 1)^{p-1} = (X+Y)^{p-1}$ en posant $X = \alpha_1(x-1)$ et $Y = \alpha_2(y-1)$. On peut supposer que $\alpha_1 \neq 0$ et $\alpha_2 \neq 0$, et alors $kG = k[X,Y]/(X^p, Y^p)$. Le reste est un calcul.