Extensions de Galois commutatives et non commutatives

Index

1 Généralités et définition

Soit A un anneau et G un sous-groupe fini des automorphismes de A. Il y a deux anneaux associés à une telle situation:

$$A^G = \{a \in A \ / \ g(a) = a \forall g \in G\}$$

$$A * G = \oplus_{g \in G} A.g$$

La multiplication de A^G est induite par celle de A, la multiplication dans $A * G$ est définie par

$$(a.g)(b.h) := ag(b).gh \quad a, b \in A, \quad g, h \in G$$

L'anneau A est évidemment un A^G-bimodule, mais en fait, la multiplication dans $A * G$ est définie de façon telle que l'application

$$A * G \to End_{A^G}(A_{A^G})$$

qu'identifie chaque élément de A avec la multiplication (à gauche) par cet-élément-là, et les éléments de G avec des éléments de $Aut(A) \subset End(A)$, soit, en fait, un morphisme d'anneaux. Par ce morphisme d'anneaux, A devient un $A*G$-A^G-bimodule. Autrement dit, si $x \in A$, $b \in A^G$ et ag est un élément de $A.g$, la structure de bimodule de A est donnée par la formule

$$ag.x.b := ag(x)b = ag(xb)$$

Dans [C-F-M], Fischman-Montgomery-Cohen ont mis en évidence l'existence d'un contexte de Morita 'naturel' entre A^G et $A*G$. Les bimodules du contexte sont tous les deux égaux à A, mais avec des structures différentes. La première étant celle décrite précédemment, la seconde donnée par:

$$b.x.ag := b(g^{-1}(xa)) = g^{-1}(bxa)$$

où on a gardé les notations d'avant, c'est-à-dire, $x \in A$, $b \in A^G$, $ag \in A.g$.

Un calcul de routine est la preuve du lemme suivant:

Lemme 1.1 *Soit A un anneau, G un sous-groupe fini des automorphismes de A. On note $tr : A \to A^G$ le morphisme de trace défini par $tr(a) = \sum_{g\in G} g(a)$. Alors, les morphismes suivants sont bien définis, et fournissent un contexte de Morita entre A^G et $A*G$:*

$$Tr : A \otimes_{A*G} A \to A^G$$

$$(a \otimes b) \mapsto tr(ab)$$

$$\beta : A \otimes_{A^G} A \to A*G$$

$$(a \otimes b) \mapsto \sum_{g\in G} ag(b).g$$

On se pose la question de quand est-ce que ce contexte-là est une équivalence. La réponse n'est qu'une application particulière de la théorie de Morita, et elle est recollée dans la proposition suivante:

Proposition 1.2 *Soit A un anneau, G un sous-groupe fini d'automorphismes de A. Les conditions suivantes sont équivalentes:*

1. *Les foncteurs $A \otimes_{A^G} (-)$ et $A \otimes_{A*G} (-)$ sont des équivalences entre les catégories de A^G-modules et $A*G$-modules, l'un étant quasi-inverse de l'autre.*

2. *Le foncteur $A \otimes_{A*G} - : A^G\text{-mod} \to A*G\text{-mod}$ est une équivalence de catégories.*

3. *Le foncteur $(-)^G : A*G\text{-mod} \to A^G\text{-mod}$ est une équivalence de catégories.*

4. *A_{A^G} est A^G-projectif de type fini et A^G-générateur, et le morphisme de structure $A*G \to End_{A^G}(A_{A^G})$ est un isomorphisme.*

5. *${}_{A*G}A$ est $A*G$-projectif et générateur.*

6. *Les morphismes $Tr : A \otimes_{A*G} A \to A^G$ et $\beta : A \otimes_{A^G} A \to A*G$ sont des isomorphismes.*

7. *Les morphismes Tr et β sont surjectifs.*

8. *Il existe un élément $a \in A$ tel que $tr(a) = 1$ et un élément $\sum_i a_i \otimes b_i \in A \otimes_{A^G} A$ tel que $\beta\left(\sum_i a_i \otimes b_i\right) = 1_{A*G}$.*

9. *Il existe un élément $a \in A$ tel que $tr(a) = 1$ et des éléments a_i, b_i ($i \in I$ un ensemble fini) tels que pour tout $g \in G$, $\sum_{i\in I} a_i g(b_i) = \delta_{id,g}$ (le delta de Krönecker).*

La preuve de cette proposition est sans malice, on va seulement l'esquisser.

D'après la théorie de Morita, si C est un anneau et P_C est un C-module à droite (et donc $End_C(P)$-C-bimodule), l'on pose $B := End_C(P)$. Le foncteur $P \otimes_C (-)$ est une équivalence si et seulement si ou bien P est C-projectif de type fini générateur, ou bien P est B-projectif de type fini générateur, ou bien $Hom_B(P, -)$ est une équivalence (Voir par exemple [A-F]).

Dans notre cas, les conditions de projectivité et génération sont respectivement 4 et 5. (On remarque qu'on a bien identifié $A^G \cong End_{A*G}({}_{A*G}A)$, et que l'isomorphisme $A * G \cong End_{A^G}(A_{A^G})$ fait partie de la condition 4.)

La partie concernant le foncteur $P \otimes_C -$ correspond biensûr à 2, le foncteur $Hom_{A*G}(A, -)$ s'identifie canoniquement à $(-)^G$ (donc 3).

$1 \Leftrightarrow 6$ est claire. $6 \Leftrightarrow 7$ est aussi bien connu (voir par exemple [A-F]). Comme β et Tr sont des morphismes de bimodules, leurs images sont des idéaux bilatères, et ça montre $7 \Leftrightarrow 8$. Finalement $8 \Leftrightarrow 9$ n'est autre chose qu'une récriture de la même chose.

Définition 1.3 *Soit A un anneau et G un sous-groupe fini d'automorphismes de A. Nous dirons que A est une* **extension Galoisienne** *de A^G si et seulement si l'une des conditions de la proposition 1.2 est satisfaite.*

1.1 Extensions de corps

Soient E un corps, G un sous-groupe fini des automorphismes de corps de E, et $F := E^G$. D'autre part, comme E n'a pas d'idéaux bilatères non triviaux, et comme en plus il est commutatif, les automorphismes (sauf l'identité) ne sont pas intérieurs. D'après le théorème qu'on trouve dans [Mo] (voir ici Théorème 5.1), l'anneau $E * G$ est simple. Le morphisme d'anneaux $E * G \to End_F(E)$ est en fait un morphisme de F-algèbres, et on sait aussi que $dim_F(E) = |G|$. Comme $E * G$ est simple, ce morphisme-là est injectif, mais les deux algèbres ont la même dimension (sur F), donc c'est un isomorphisme. On remarque aussi que comme $F = E^G$ est un sous-corps, E est un F-module libre (donc projectif générateur).

On a vu alors qu'une extension Galoisienne finie 'classique' de corps est toujours une extension Galoisienne au sens de la définition 1.3.

1.2 Anneaux intègres

Soit A un anneau commutatif intègre et G un sous-groupe fini d'automorphismes de A. On ne sait pas si l'extension $A|A^G$ est Galois, mais on peut regarder $E := frac(A)$, le corps de fractions de A.

Un élément de E est une fraction a/b avec a, $b \in A$, $b \neq 0$. Si on multiplie numérateur et dénominateur par $\prod_{g \in G - \{id\}} g(b)$ on se rend compte que on peut se ramener toujours à une fraction avec dénominateur dans A^G. On voit de cette manière que $E = (A^G - \{0\})^{-1}A$, et que si $F := E^G$, $F = frac(A^G)$.

Sans hypothèses sur le sous-groupe G, on sait que l'extension $E|E^G$ est Galois, alors il existe $x_i, y_i \in E$ tels que

$$\sum_{i \in I} x_i g(y_i) = \delta_{eg}$$

Comme on peut écrire chaque $x_i = a_i/\lambda_i$, $y_i = b_i/\mu_i$, avec λ_i et μ_i dans $A^G - \{0\}$, on voit que ces équations sont valables déjà dans une localisation intermédiaire entre A et E. Par exemple dans $A[f^{-1}]$, où $f := (\prod_i \lambda_i).(\prod_i \mu_i)$.

On a donc prouvé:

Proposition 1.4 *Soit A un anneau commutatif intègre et G un sous-groupe fini d'automorphismes de A. Alors il existe $f \in A^G$ tel que $A[f^{-1}]$ est une extension Galois de $A[f^{-1}]^G$.*

1.3 La trace et les a_i, b_i

Proposition 1.5 *A un anneau, G un groupe fini d'automorphismes de A.*

- *${}_{A*G}A$ est $A*G$ projectif si et seulement si il existe un élément a tel que $tr(a) = 1$*
- *${}_{A*G}A$ est $A*G$ générateur si et seulement si il existe des éléments a_i, b_i tels que pour tout $g \in G$: $\sum_{i \in I} a_i g(b_i) = \delta_{id,g}$.*

Du point de vue de A comme A^G-module on a l'énoncé "dual":

- *${}_{A^G}A$ est A^G projectif si et seulement si il existe des éléments a_i, b_i tels que pour tout $g \in G$: $\sum_{i \in I} a_i g(b_i) = \delta_{id,g}$.*
- *A^G est un summand direct de ${}_{A^G}A$ si et seulement si il est un summand direct de A_{A^G}, si et seulement si il existe $a \in A$ tel que $tr(a) = 1$.*

Finalement, A^G es un summand direct de A comme A^G-bimodule si et seulement si il existe $a \in \mathcal{Z}(A)$ tel que $tr(a) = 1$.

La preuve de cette proposition est facil. Par example, la condition de projectivité de A comme $A*G$ module provient de regarder le morphisme $\epsilon : A*G \to A$ $(ag \mapsto a)$. Les autres parties sont égalément faciles, c'est de la verification immédiate.

1.4 Générateurs de A et A^*

Comme on a pu voir dans la proposition 1.5, il y a des propriétés de l'anneau A qui dépendent 'séparément' de la condition ou bien de trace, ou bien des a_i, b_i. Voilà un deuxième exemple, qui en fait sera utilisé pour démontrer que la partie d'existence d'un élément de trace un est superflue lorsque A est commutatif intègre.

Proposition 1.6 *Soit A un anneau, G un sous-groupe fini d'automorphismes de A tels qu'il existe a_i, b_i des éléments dans A vérifiant $\sum_i a_i g(b_i) = \delta_{id,g}$. Alors*

1. *Les a_i sont un ensemble de générateurs de A_{A^G}, les b_i sont un ensemble de générateurs de ${}_{A^G}A$, les fonctions $tr(b_i.-)$ sont des générateurs de $Hom_{A^G}(A_{A^G}, A^G)$, et les fonctions $tr(-.a_i)$ sont des générateurs de $Hom_{A^G}({}_{A^G}A, A^G)$.*
2. *l'application $a \mapsto tr(a.-)$ donne un isomorphisme ${}_{A^G}A \cong Hom_{A^G}(A_{A^G}, A^G)$.*

Preuve: 1. Si $x \in A$,

$$x = \sum_{g \in G} \delta_{id,g} g(x) = \sum_i \sum_{g \in G} a_i g(b_i) g(x) = \sum_i a_i tr(b_i.x)$$

On obtient alors que A est engendré à droite par les a_i, et que $tr(b_i.-)$ est une 'base projective' duale aux a_i, *ergo* $tr(b_i.-)$ est un système de générateurs de $Hom_{A^G}(A_{A^G}, A^G)$. En considérant A^{op} on montre le reste de l'assertion.

2. Soit $a \in A$ tel que $tr(a.x) = 0$ pour tout $x \in A$, en particulier

$$0 = \sum_i tr(a.a_i) b_i = \sum_{g \in G} \sum_i g(a) g(a_i) b_i = \sum_{g \in G} g(a) \delta_{id,g^{-1}} = a$$

Ce qui montre que l'application $a \mapsto tr(a.-)$ est injective. Considérons maintenant $f \in Hom_{A^G}(A_{A^G}, A^G)$ et $x \in A$,

$$f(x) = \sum_i f(a_i tr(b_i x)) = \sum_i f(a_i) tr(b_i x) = \sum_i tr(f(a_i) b_i x) = tr\left((\sum_i f(a_i) b_i).x \right)$$

Cela montre que f est de la forme $tr(b.-)$, avec $b = \sum_i f(a_i) b_i$.

2 Conséquences immédiates

2.1 Morphismes

À partir de la condition avec les éléments a, a_i et b_i de la définition de Galois, on déduit de manière élémentaire le fait suivant:

Proposition 2.1 *Soient A et B deux anneaux, G un groupe qui agit par automorphismes d'anneau dans A et B. Supposons qu'il existe un morphisme d'anneaux $f : A \to B$ qui commute avec l'action de G. Alors, si l'extension $A|A^G$ est Galois, il en est de même pour $B|B^G$*

Preuve: Si $a, a_i, b_i \in A$ sont des éléments qui vérifient $tr(a) = 1$, $\sum_i a_i g(b_i) = \delta_{id,g}$, on prend les éléments $f(a)$, $f(a_i)$ et $f(b_i)$.

On va illustrer cette proposition dans quelques cas particuliers:

1. Localisation. Soit $S \subset \mathcal{Z}(A)$ une partie multiplicative G-stable. La localisation $A \to A_S$ est G-équivariante, alors (A, G) Galois implique (A_S, G) Galois.
2. Anneaux gradués. Soit $A = \oplus_{n \geq 0} A_n$ un anneau $\mathbb{Z}$-gradué et G un groupe fini d'automorphismes de A qui respectent la graduation. Alors, A est une extension Galoisienne de A^G si et seulement si A_0 est une extension Galois de A_0^G.
3. Idéaux stables. Si $I \subset A$ est un idéal bilatère G-stable, la projection $A \to A/I$ est G-équivariante. Comme cas particulier on a $rad(A) = J(A)$ l'idéal de Jacobson de A, c'est-à-dire l'intersection de tous les idéaux maximaux à gauche de A, qui est en fait un idéal bilatère, et qui coïncide avec l'intersection de tous les idéaux maximaux à droite de A. $rad(A)$ est toujours un idéal G-stable, mais dans ce cas-ci on a (A, G) Galois si et seulement si $(A/rad(A), G)$ Galois. La preuve de ce fait provient du fait d'avoir une unité de la forme $1 + r$ dans l'image de Tr et de β.
4. Extensions de scalaires. Soit k un sous-anneau du $\mathcal{Z}(A)$ et B une k-algèbre. Alors (A, G) Galois implique $(A \otimes B, G)$ Galois. De plus, si B est fidèlement plat sur k, (A, G) Galois si et seulement si $(A \otimes B, G)$ Galois.

   Preuve: On peut identifier alors $(A \otimes_k B)^G$ avec $A^G \otimes_k B$. De plus, $(A \otimes_k B) * G = (A * G) \otimes_k B$, et les morphismes

   $$Tr : (A \otimes_k B) \otimes_{(A*G)\otimes_k B} (A \otimes_k B) = (A \otimes_{A*G} A) \otimes_k B \to (A^G) \otimes_k B$$

   $$\beta : (A \otimes_k B) \otimes_{A^G \otimes_k B} (A \otimes_k B) = (A \otimes_{A^G} A) \otimes_k B \to (A * G) \otimes_k B$$

   s'identifient naturellement à $Tr \otimes id$ et $\beta \otimes id$. Comme on a suppose B fidèlement plat sur k, les morphismes $Tr \otimes id$ et $\beta \otimes id$ sont des épimorphismes si et seulement si Tr et β sont des épimorphismes.
   Application: k un corps, $B = \overline{k}$.

2.2 Sous-groupes

Proposition 2.2 *Soit A un anneau quelconque, G un sous-groupe fini d'automorphismes de A, et $H \subseteq G$ un sous-groupe de G.*

- *Si (A, G) est Galois, alors (A, H) est Galois.*
- *Si $H \triangleleft G$ est un sous-groupe normal de G, comme H agit trivialement sur A^H alors G/H agit sur A^H. De plus, si (A, G) est Galois, alors $(A^H, G/H)$ est Galois.*

La preuve est facil. Par example pour la deuxième partie, on utilise la fonction $tr_H : A \to A^H$ pour trouver, à partir des a_i, b_i dans A, des $\widetilde{a_i}$ et $\widetilde{b_i}$ dans A^H; ces elements-là marchent (modulo multiplication par $tr_H(a)$, où $a \in A$ est tel que $tr_G(a) = 1$).

2.3 Le théorème de Maschke

Soit maintenant A un anneau, et G un sous-groupe fini d'automorphismes de A.

Sous certaines conditions on a un théorème de Mashcke:

Proposition 2.3 *Supposons qu'il existe* $a \in \mathcal{Z}(A)$ *tel que* $tr(a) = 1$. *Si* $f : M \to N$ *est un morphisme de* $A * G$ *modules qui admet une section (resp. rétraction)* A*-linéaire, alors* f *admet une section (resp. rétraction)* $A * G$*-linéaire.*

Preuve: il n'y a pas de surprises, on 'moyenne' les morphismes pour qu'ils deviennent G-linéaires. Si f est un morphisme entre deux $A * G$-modules qui est A-linéaire, alors $\sum_{g \in g} g^{-1}(f(ga.-))$ est $A * G$-lineaire, et cela définit une projection du Hom_A vers Hom_{A*G}.

Corollaire 2.4 *On garde les notations précédentes, soit* $a \in \mathcal{Z}(A)$ *tel que* $tr(a) = 1$ *et* M *un* $A * G$*-module. Alors*

- M *est* $A * G$*-projectif si et seulement si* M *projectif comme* A*-module.*
- M *est* $A * G$*-injectif si et seulement si* M *injectif comme* A*-module.*

et en conséquence

- $projdim_{A*G}(M) = projdim_A(M)$
- $injdim_{A*G}(M) = injdim_A(M)$

En particuliér, $lgldim(A) = lgldim(A * G)$ *et* $injdim_A(A) = injdim_{A*G}(A * G)$.

On fait la preuve sur la partie de la dimension injective.

Si l'on considère M un $A * G$-module et une résolution $A * G$-injective, comme un $A * G$-module est injectif si et seulement si il est A-injectif alors $injdim_{A*G}(M) \geq injdim_A(M)$.

Réciproquement, étant donné M un $A * G$-module, si $injdim_A(M) = n < \infty$, soit I_* une résolution $A * G$-injective de M, alors c'est une résolution A-injective, et comme $injdim_A(M) = n$ on sait que $Im(d_n)$ est un module A-injectif, donc $A * G$-injectif. Cela montre que $injdim_{A*G}(M) \leq injdim_A(M)$.

Maintenant, pour $M = A * G$:

$$injdim_{A*G}(A * G) = injdim_A(A * G) = injdim_A(\oplus_{g \in G} A.g) = injdim_A(A)$$

Corollaire 2.5 *Soit* (A, G) *Galois admettand* $a \in \mathcal{Z}(A)$ *avec* $tr(a) = 1$. *Alors*

- *(régularité)* $lgldim(A^G) = lgldim(A)$.
- *(Gorenstein)* $injdim_{A^G}(A^G) = injdim_A(A)$.

Preuve: Comme A^G est Morita équivalent à $A * G$ et la dimension globale projective (à gauche) est un invariant Morita, on a $lgldim(A^G) = lgldim(A * G) = lgldim(A)$, et cela montre le résultat de régularité.

Concernant la propriété de Gorenstein, l'équivalence de Morita nous donne $injdim_{A^G}(A^G) = injdim_{A*G}(A \otimes_{A^G} A^G) = injdim_{A*G}(A) = injdim_A(A)$.

Remarque: La condition A régulier et A^G régulier n'est pas suffisante pour assurer que l'extension est Galois.

Exemple: Soit k un corps de caractéristique différente de 2, $A = k[x]$ et $G = \mathbb{Z}/2\mathbb{Z}$. Soit g générateur de G, on définit l'action par $g(x) = -x$.

Dans ce cas-ci, il est clair que $A^G = k[x^2]$ qui est un anneau de polynômes, aussi régulier que A. Comme on suppose $ch(k) \neq 2$ la trace est un épimorphisme, on regarde maintenant le morphisme $\beta : A \otimes_{A^G} A \to A * G$.

L'ensembre $\{1, x\}$ est une base de A comme A^G-module, donc tout élément de $A \otimes_{A^G} A$ peut s'écrire (de façon unique) sous la forme $p \otimes 1 + q \otimes x$, avec $p, q \in A$. Pour voir si $1 \in Im(\beta)$ il faut résoudre le système d'équations

$$p + qx = 1$$
$$p - qx = 0$$

C'est un système linéaire, on cherche les solutions de façon élémentaire. Par exemple, on peut le voir comme deux équations à coefficients appartenant au corps $k(x)$. Le déterminant du système est $-2x$, et il a donc une solution unique dans $k[x, x^{-1}]$. Si par hasard cette unique solution se trouve dans $k[x]$, l'extension sera Galoisienne, sinon, non. Mais la solution est $p = \frac{1}{2}$, $q == \frac{1}{2x}$, qui n'est pas dans $k[x]$, et donc A n'est pas une extension Galois de A^G. Par contre, G agit sur $k[x, x^{-1}]$ et $k[x, x^{-1}]$ est une extension Galois de $k[x, x^{-1}]^G = k[x^2, x^{-2}]$, où $b_1 = 1$, $b_2 = x$, $a_1 = \frac{1}{2}$ et $a_2 = \frac{1}{2x}$.

Exemple: Soit $A = k[x_1, \ldots, x_n]$, $G = \S_n$ le groupe de permutations, agissant sur A par permutation des x_i's. Il est bien connu que $A^G = k[s_1, \ldots, s_n]$ est une algèbre de polynômes dans les fonctions symétriques élémentaires et est évidemment régulière. On serait tenté de dire que l'extension est Galoisienne, mais si l'on considère la permutation cyclique $\sigma = (1, 2, \ldots, n)$ (qui n'est pas une pseudoreflection) la sous-extension A^σ est une algèbre singulière, donc (A, G) ne peut pas être Galois.

Par contre, si on localise par l'élément $\delta := \prod_{i<j}(x_i - x_j)$, alors $(A[\delta^{-1}], G)$ est Galois.

3 Sur la trace dans les anneaux intègres

Le but de cette section est de montrer que si A est un anneau intègre, et G un sous-groupe fini d'automorphismes de A tel qu'il existe des a_i, b_i dans A vérifiant $\sum_i a_i g(b_i) = \delta_{id,g}$ $(\forall g \in G)$, alors A est une extension galoisienne de A^G. Autrement dit, l'existence des a_i, b_i implique, quand A est intègre, l'existence d'un élément de trace un.

Ce résultat a été prouvé avec un peu plus de généralité dans [C-H-R] utilisant une hypothèse sur les idempotents (toujours dans le cas commutatif), mais ils ne donnent pas d'exemple. On trouve aussi dans [Fe] une condition (exprimée en termes des idempotents) pour avoir un enoncé analogue dans le cas non commutatif. Tout de même, il paraît que cette propriété est bien particulier des algèbres commutatives intègres, puisque on verra plus tard avec un contre-exemple de cet enoncé avec $G = \mathbb{Z}/2\mathbb{Z}$ et $A = M_3(k)$ où k un corps de caractéristique 2.

La preuve du théorème repose sur le fait suivant:

Lemme 3.1 *Soit R un anneau commutatif, M un R-module de type fini, J un idéal de R. Alors $J.M = M$ si et seulement si $R = J + Ann(M)$.*

Corollaire 3.2 *Soit R commutatif et intègre, M un R-module projectif de type fini, alors M est un générateur. Autrement dit, l'image du morphisme canonique $ev : M^* \otimes_R M \to R$ est R tout entier.*

Maintenant le théorème annoncé:

Théorème 3.3 *Soit A un anneau intègre et G un sous-groupe fini d'automorphismes de A. On suppose qu'il existe des $a_1, \ldots, a_n, b_1, \ldots, b_n$ dans A vérifiant, pour tout $g \in G$, $\sum_{i=1}^n a_i g(b_i) = \delta_{id,g}$. Alors, il existe un élément $a \in A$ tel que $\sum_{g \in G} g(a) = 1$.*

Preuve: on est en condition d'utiliser la proposition 1.6. Pour sa première partie on sait que A est A^G-projectif de type fini.

Grâce au corollaire précédent, l'image de l'évaluation $A^* \otimes_{A^G} A \to A$ contient 1, il existe donc $p_i \in A^*$, $x_i \in A$ tels que $\sum_{i=1}^n p_i(x_i) = 1$.

On utilise une deuxième fois la proposition 1.6, pour le point 2 on sait que l'application $A \to A^*$ donnée par $a \mapsto tr(a.-)$ est une bijection, alors chaque p_i est de la forme $tr(y_i.-)$, donc finalement

$$1 = \sum_{i=1}^n p_i(x_i) = \sum_{i=1}^n tr(y_i.x_i) = tr\left(\sum_{i=1}^n y_i x_i\right)$$

On prend $a := \sum_{i=1}^n y_i x_i$ et la preuve est finie.

4 Extensions de Galois d'anneaux commutatifs

4.1 Caractérisation en termes d'idéaux maximaux

Quand l'anneau A est commutatif, on peut regarder la condition de Galois en termes d'idéaux maximaux. La proposition suivante provient de [D-I]:

Théorème 4.1 *Soit A un anneau commutatif, G un sous-groupe fini d'automorphismes de A. Les deux conditions suivantes sont équivalentes:*

1. *Il existe des a_i, b_i tels que pour tout $g \in G$, $\sum_{i\in I} a_i g(b_i) = \delta_{id,g}$.*
2. *Pour tout idéal maximal $\mathcal{M}$ et pour tout $g \in G$, il existe $x \in A$ tel que $x - g(x) \notin \mathcal{M}$.*

Remarques: Si $g \in G$, on peut définir l'idéal $I_g = \langle x - g(x) \ : \ x \in A\rangle \subseteq A$. La condition 2 du théorème équivaut à dire que $I_g = A$ pour tout $g \neq 1$.

2. Si F est un corps, G un groupe fini d'automorphismes de F, et $g \in G$ différent de l'identité, il est clair qu'il existe $x \in F$ tel que $x - g(x) \neq 0$. Après ce théorème on voit pour la deuxième fois que tout corps est une extension Galois de ses invariants.

La preuve proposée est essentiellement identique à celle de [D-I], sauf qu'on a choisi d'écrire sous forme de lemme l'argument principal, parce que de cette façon on obtiendra un corollaire intéressant qui n'est pas mentionné dans la littérature.

Lemme 4.2 *Soit A un anneau commutatif et g un automorphisme de A. Si l'idéal engendré par les éléments de la forme $x - g(x)$ coïncide avec A, alors il existe des éléments de A, a_i, b_i, ($i \in I$ un ensemble fini) tels que $\sum_{i\in I} a_i b_i = 1$ et $\sum_{i\in I} a_i g(b_i) = 0$.*

Preuve: Par hypothèse, l'idéal engendré par les éléments de la forme $(x - g(x))$ est égal à A, alors il existe des x_i, y_i, $i = 1, ..., n$ tels que $1 = \sum_{i=1}^n x_i(y_i - g(y_i))$. On peut récrire cette formule de la façon suivante:

$$1 = \sum_{i=1}^n x_i y_i + \left(\sum_{i=1}^n x_i g(y_i)\right).(-1)$$

On prend $a_i = x_i$, $b_i = y_i$, $i = 1, ..., n$, $a_{n+1} := \sum_{i=1}^n x_i g(y_i)$, $b_{n+1} = -1$. Avec ces changements de notations on a

$$\sum_{i=1}^{n+1} a_i b_i = 1$$

mais aussi

$$\sum_{i=1}^{n+1} a_i g(b_i) = \sum_{i=1}^n a_i g(b_i) + a_{n+1} g(b_{n+1}) = \sum_{i=1}^n x_i g(y_i) + \left(\sum_{i=1}^n x_i g(y_i)\right).g(-1) = 0$$

Maintenant, un lemme de recollement.

Lemme 4.3 *Soit A un anneau commutatif, g et h deux automorphismes de A. Supposons qu'il existe des éléments a_i, b_i, a'_j, b'_j tels que*

$$\sum_{i\in I} a_i b_i = 1 \ ; \ \sum_{j\in J} a'_j b'_j = 1$$

$$\sum_{i\in I} a_i g(b_i) = 0 \ ; \ \sum_{j\in J} a'_j h(b'_j) = 0$$

Alors, on peut trouver des éléments a''_k, b''_k qui ont les mêmes propriétés pour h et g simultanément, plus précisément, vérifiant $\sum_{k\in K} a''_k b''_k = 1$, $\sum_{k\in K} a''_k g(b''_k) = 0$ et $\sum_{k\in K} a''_k h(b''_k) = 0$.

Preuve: On définit d'abord l'ensemble d'indice $K := I \times J$, et pour chaque $k \in K$,

$$a''_{ij} := a_i a'_j$$

$$b''_{ij} := b_i b'_j$$

et cela marche. On remarque que pour faire les calcules on utilise la commutativité de A.

La preuve du théorème 4.1 est déjà presque fini:

$1 \Rightarrow 2$.

Soit $\mathcal{M}$ un idéal maximal, $g \in G$, si $x - g(x) \in \mathcal{M}$ pour tout x, on a en particulier que $1 = 1 - 0 = \sum_i a_i(b_i - g(b_i)) \in \mathcal{M}$, ce qui est absurde.

$2 \Rightarrow 1$.

Soit $g \in G$, $g \neq id$ et considérons l'idéal engendré par les éléments de la forme $x - g(x)$. Par hypothèse, il n'est contenu dans aucun idéal maximal, donc il coïncide avec A.

D'après le premier lemme, on peut trouver des éléments a_i, b_i (qui éventuellement dépendent de g) qui vérifient la condition $\sum_i a_i b_i = 1$ et $\sum_i a_i g(b_i) = 1$. Mais le deuxième lemme nous dit comment récoller les éléments correspondant à chaque g pour avoir la même formule pour les différents g, mais avec le même paquet d'éléments a_i, b_i.

Exemple: Soit $A = k[x_1, ...x_n]$ et G un sous-groupe fini non trivial de $Gl(n, k)$. Alors l'action de G dans A n'est jamais Galois.
Preuve: soit $\mathcal{M} = \langle x_1, \ldots, x_n \rangle$. Si p est un pôlynome, et $g \in G$, alors $p(0) = g(p)(0)$ et cela montre que $p - g(p) \in \mathcal{M}$ pour tout $p \in A$.

4.2 Sous-groupes cycliques

En revanche, voici un résultat positif:

Proposition 4.4 *Soit A un anneau commutatif intègre et G un sous-groupe fini d'automorphismes de A. Alors l'extension $A|A^G$ est Galois, si et seulement si pour tout sous-groupe cyclique $C \subseteq G$, l'extension $A|A^C$ est Galois.*

Exemple: Soit $A := k[a, b, c, d]/\langle ad - bc - 1 \rangle$, l'algèbre des fonctions régulières sur $SL(2, k)$. Soit G un sous-groupe fini $SL(2, k)$, et on suppose aussi que k est un corps de caractéristique zéro. En réalité, l'exemple reste tel quel si l'on suppose que l'ordre de G est inversible dans k.

Le groupe G agit sur $SL(2, k)$ par translation à gauche, et donc agit par automorphismes d'algèbre sur A. Par exemple, si $g \in G$ est une matrice $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$, l'action de g sur les générateurs de A est donnée par:

$$g(a) = xa + yc \quad ; \quad g(b) = xb + yd$$

$$g(c) = za + tc \quad ; \quad g(d) = zb + td$$

On affirme que cette action est *toujours* Galoisienne.
Preuve: D'après la proposition, il suffit de voir que l'extension associée à chaque sous-groupe fini est Galois. On suppose alors, sans perte de généralité, que le groupe G est cyclique, engendré par un élément g. Après la propriété par rapport aux extensions fidèlement plat et considérant la clôture algébrique de k, on peut supposer aussi que k contient toutes les racines $|g|$-ièmes de l'unité, donc g est diagonalisable. Après un isomorphisme de "changement de base" on suppose g diagonal c'est-à-dire, $g = \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix}$, où w est une racine $|g|$-ième primitive de l'unité. On réécrit la formule de l'action pour un tel g:

$$g(a) = wa \quad ; \quad g(b) = wb$$

$$g(c) = w^{-1}c \quad ; \quad g(d) = w^{-1}d$$

Si on définit l'idéal $I_g := \langle x - g(x) \ : \ x \in A\rangle$, il faut voir qu'il contient l'élément 1.

On prend $x_1 = a$, $x_2 = b$, alors $x_1 - g(x_1) = (1-w)a$, $x_2 - g(x_2) = (1-w)b$. Cela montre que $a, b \in I_g$, et alors $1 = ad - bc \in I_g$.

On verra dans la sous-section suivante, une généralisation de ce résultat, pour une algèbre de Hopf commutative de type fini au lieu de l'anneau de fonctions sur $SL(2,k)$

Le théorème 4.1 donne une interprétation géométrique de la condition Galois. On peut définir le sous-ensemble de maximaux:

$$\mathcal{Z} := \{\mathcal{M} \subset A \text{ idéal maximal } / \exists g \in G \text{ avec } \langle (x - g(x)) : x \in A\rangle \subseteq \mathcal{M}\}$$

Par définition même, Z est un fermé Zariski de $\mathrm{SpecMax}(A)$, en fait $Z = \cup_{g\in G}\mathcal{V}(I_g)$ où $I_g = \langle (x - g(x)) \ : \ x \in A\rangle$.

Avec cette notation, A est une extension Galois de A^G si et seulement si $\mathcal{Z} = \emptyset$, si et seulement si $\mathcal{V}(g) = \emptyset$ pour tout $g \in G$. Dans le cas général, on sait que, si A est intègre, alors $\mathcal{Z}$ est contenu dans une hypersurface de $SpecMax(A)$ (voir proposition 1.4), alors le complément de $\mathcal{Z}$ est toujours un ouvert non vide. Si A est régulier, l'ensemble $\mathcal{Z}/G \in \mathrm{SpecMax}(A^G)$ est un fermé que contient le fermé de points singuliers de A^G (voir corollaire 2.5).

4.3 Action par translation d'un sous-groupe fini d'un groupe affine

Le but de cette sous-section sera de montrer que si G est un sous-groupe fini d'un groupe algébrique affine, alors l'action de G par translation définit, sur l'anneau du groupe algébrique, une action qui est toujours Galoisienne.

L'enoncé du théorème est le suivant:

Théorème 4.5 *Soit H une k-algèbre de Hopf commutative de type fini (comme k-algèbre), et $\pi : H \to k^{(G)}$ un épimorphisme d'algèbres de Hopf (G un groupe fini). On assume aussi, soit $ch(k) = 0$ ou soit H intègre (i.e. le groupe algébrique associe à H connexe). Alors, avec l'action de G obtenue à partir de la structure de $k^{(G)}$-comodule donnée par π (i.e. $\rho^+ = (id \otimes \pi) \circ \Delta : H \to H \otimes k^{(G)}$), on a que H est une extension Galoisienne de H^G.*

Remarques: Grâce à la propriété par rapport aux extensions fidèlement plates et considérant (si nécessaire) $\overline{k}^{(G)}$ et $H \otimes_k \overline{k}$, on peut supposer sans perte de généralité que k est algébriquement clos.

On va utiliser la caractérisation d'extension Galois donnée par le théorème 4.1. La preuve est divisée en deux lemmes, mais avant les lemmes, on voit bien que si $\pi : H \to k^{(G)}$ est un morphisme d'algèbres de Hopf, alors H est une $K^{(G)}$-comodule algèbre. L'action d'un élément de g sur un élément a de A est définie par

$$g(a) = a_0.a_{+1}(g) = a_1.\pi(a_2)(g)$$

Un épimorphisme d'algèbres de Hopf $H \to k^{(G)}$ correspond à une inclusion de G dans le spectre maximal de H, c'est-à-dire à un sous-groupe fini du groupe algébrique affine défini par H. La comultiplication dans une algèbre de Hopf se correspond avec la multiplication du groupe, alors dans notre cas, le morphisme de structure de H comme $k^{(G)}$-comodule se corresponde avec la multiplication par des éléments de G, c'est-à-dire avec l'action par translation.

Lemme 4.6 *Mêmes hypothèses que dans le théorème 4.5 et l'on assume $k = \overline{k}$.*

1. *Si $\mathcal{M}$ est un idéal maximal de H, et $g \in G$, alors $g^{-1}(\mathcal{M}) = \mathcal{M}$ si et seulement si $\epsilon = \epsilon \circ g$.*
2. *si $g \in G$, $g \neq e$ alors $\epsilon \circ g \neq \epsilon$.*

Remarque: D'après ces deux lemmes, la preuve du théorème est presque évident. Si on choisit $\mathcal{M}$ un ideal maximal et $g \neq e$ alors $g(\mathcal{M}) \neq \mathcal{M}$ et donc il existe un élément $m \in \mathcal{M}$ tel que $g(m) \notin \mathcal{M}$, alors $m - g(m)$ n'appartient pas à $\mathcal{M}$ non plus.

5 Anneaux simples

5.1 Simplicité des produits croisés

On rappelle ici un théorème sur les anneaux simples qu'on trouve dans le Lect.N.M de Montgomery sur les anneaux d'invariants [Mo]:

Théorème 5.1 *Soit A un anneau simple et G un sous-groupe d'automorphismes de A tel qu'il ne contient pas d'automorphisme intérieure, sauf l'identité. Alors $A * G$ est simple.*

Preuve: Soit $I \subset A * G$ un idéal bilatère non nul. Si $x \in I$, $x = \sum_{g \in G} x_g.g$ (somme à support fini), on prend $x \neq 0$ dans I tel que son support ait cardinal minimum.

On choisit $g \in sup(x)$, et en changeant -si necessaire- x par $x.g^{-1}$ on peut supposer que $e = 1_G \in supp(x)$, on écrit x sous la forme

$$x = x_e.e + \sum_{g \neq e} x_g.g$$

avec $x_g \in A$, $x_e \neq 0$.

Comme A est simple et $x_e \neq 0$, l'idéal engendré par x_e est égal à A, donc il existe $a_i, b_i \in A$ tels que $\sum_{i \in I} a_i x_e b_i = 1$. On peut changer (sans agrandir le support) x par $\sum_{i \in I} a_i x b_i$ et supposer, sans perte de généralité, que $x_e = 1$.

Si $supp(x) = e$ alors $x = 1 \in I$ et $I = A$, on a fini. Sinon, soit $a \in A$ un élément arbitraire, comme $(ax - xa) \in I$ et $supp(ax - xa) \subset (sup(x) - \{e\})$, par minimalité du cardinal du support on a nécessairement

$$ax - xa = 0 = \sum_{g \neq e} (ax_g - x_g g(a))g$$

Alors, pour tout g dans le support de A on a l'égalité suivante:

$$ax_g = x_g g(a)$$

D'abord on voit que $x_g.A = A.x_g$, et donc égal à $A.x_g.A$, qui est égal a A parce que $x_g \neq 0$ et A est simple. On a prouvé ainsi que x_g est une unité, et l'on peut maintenant résoudre l'équation $ax_g = x_g g(a)$; cela donne

$$(x_g)^{-1} a x_g = g(a)$$

pour tout $g \in supp(x)$ et tout $a \in A$. Mais G n'a pas d'automorphismes intérieurs sauf l'identité, alors $g = id$ et la preuve est finie.

5.2 Surjectivité de Tr et β

On revient aux morphismes du contexte de Morita:

$$Tr : A \otimes_{A*G} A \to A^G$$

$$\beta : A \otimes_{A^G} A \to A * G$$

pour trouver des conditions faciles à vérifier qui impliquent la surjectivité de ces deux morphismes.

Comme Tr et β sont des morphismes de bimodules, leurs images sont des idéaux bilatères. La situation la plus simple possible pour voir si au moins un de ces morphismes est surjectif est quand il n'y a pas trop d'idéaux bilatères. L'exemple le plus facile est quand A est un corps. Comme un corps est commutatif, les automorphismes ne sont jamais intérieurs, d'après la proposition précédente $A * G$ est simple, alors β est surjectif. On peut ou bien utiliser le théorème de Dedekind sur l'indépendence linéaire des automorphismes différents, ce qui assure que Tr est non nul, est donc surjectif aussi. Ou bien on peut utiliser le théorème 3.3 qui nous dit que si A est intègre, la surjectivité de β implique la surjectivité de Tr.

On a tout de même un exemple non commutatif fondamental:

5.3 Exemple d'opérateurs différentiels

Soi A un anneau commutatif intègre régulier, on suppose aussi $\mathbb{Q} \subset A$. Si G est un sous-groupe d'automorphismes de A, le groupe G agit aussi dans l'algèbre d'opérateurs différentiels Diff(A). Pour des raisons de degré de filtration, il est relativement facile de voir que les uniques automorphismes intérieurs de Diff(A) sont les conjugaisons par rapport à des éléments de A. Mais comme A est commutatif, ces automorphismes intérieurs, restreints à A, donnent l'identité. Alors l'action de G sur Diff(A) (qui provient d'une action de G sur A) ne contient pas d'automorphismes intérieurs.

Comme on a supposé A intègre régulier, Diff(A) est simple, alors Diff(A) $* G$ est simple et l'on a que, sous ces hypothèses-là, Diff(A) $* G$ est *toujours* Morita équivalent a Diff$(A)^G$, c'est-à-dire, Diff(A) est une extension Galois de Diff$(A)^G$.

5.4 Exemple avec matrices 1

On remarque que l'hypothèse de G n'ayant pas d'automorphismes intérieurs n'est pas technique, mais nécessaire (en général) dans le théorème 5.1. On a l'exemple suivant:

Soit k un corps (de caractéristique arbitraire), $A := M_2(k)$, les matrices 2×2 à coefficients dans k. L'anneau A est simple (par exemple parce qu'il est Morita équivalent à k). Soit $G = \mathbb{Z}/2\mathbb{Z}$, on désigne par σ son générateur, que l'on fait agir sur A par conjugaison par rapport à la matrice

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

On remarque que $Aut_k(M_3(k)) = AutInt(M_3(k))$. (Une raison est encore l'équivalence de Morita, appliquée à $Pic_k(M_n(k)) = Pic_k(k) = \{1\}$ d'où $Aut_k(M_n(k))/InnAut(M_n(k)) = \{1\}$.)

De façon élémentaire, on voit que si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, alors $XMX = \begin{pmatrix} d & c \\ b & a \end{pmatrix}$ Les matrices invariantes sont celles qui vérifient $a = d$ et $b = c$, c'est-à-dire, celles qui sont de la forme $a.I + b.X$. Elles forment une sous-algèbre de dimension (sur k) égale à deux. On a évidemment un isomorphisme de k-algèbres $A^G \cong k[X]/(X^2 - 1)$, et comme le polynôme $X^2 - 1$ se factorise sur $\mathbb{Z}$, alors pour n'importe quel corps k, A^G n'est pas simple.

Si on calcule la trace de la matrice E_{11} (la matrice qui a des zéros partout sauf à la place 11, où il y a un 1), on obtient $tr(E_{11}) = E_{11} + XE_{11}X = E_{11} + E_{22} = I$. On voit donc que le morphisme tr est surjectif, même en caractéristique 2.

On se demande si $A * G$ est simple ou pas. Si $A * G$ est simple, alors β est surjective, et $A * G$ serait Morita équivalent a A^G. Mais A^G n'est pas simple, et la simplicité est un invariant Morita, cela serait absurde et donc $A * G$ n'est pas simple.

Tout de même, on n'a toujours pas résolu la question de savoir si A^G est Morita équivalent à $A * G$; la répose à cette question est oui.

Pour étudier la surjectivité de β on agit de la même façon que dans les exemples sur $k[x]$, c'est-à-dire, on trouve des générateures de A comme A^G-module (par exemple à droite) et ainsi on réduit l'écriture d'un élément typique de $A \otimes_{A^G} A$. Dans ce cas, si l'on considère les matrices E_{11} et E_{12}, on peut vérifier les identités suivantes:

$$XE_{11}X = E_{22} = 1 - E_{11}$$

$$XE_{12}X = E_{21} = X - E_{12}$$

$$E_{11}^2 = E_{11} \ ; \ E_{12}^2 = 0$$

$$XE_{11} = E_{21} = X - E_{12} \ ; \ E_{11}X = E_{12}$$

$$XE_{12} = E_{22} = 1 - E_{11} \ ; \ E_{12}X = E_{11}$$

En particulier, $A = I.A^G \oplus YA^G$ comme A^G-modules à droite, et tout élément de $A \otimes_{A^G} A$ peut s'écrire (et de façon unique) $I \otimes M + E_{11} \otimes N$, avec M et N dans A. Il faut résoudre alors le système d'équations:

$$M + E_{11}N = I$$

$$M + XE_{11}XN = 0$$

De la deuxième équation on tire $M = -E_{22}N$, si on remplace dans la première on a

$$-E_{22}N + E_{11}N = I$$

Et l'on voit bien que $-E_{22}N + E_{11}N = (E_{11} - E_{12})N = I$ à une solution, avec $N = E_{11} - E_{22}$. Si l'on prend maintenant $a_1 = I$, $a_2 = E_{11}$, $b_1 = -E_{22}(E_{11} - E_{22}) = E_{22}$, $b_2 = E_{11} - E_{22}$ on a les a_i, b_i qui impliquent la surjectivité de β.

5.5 Exemple avec matrices 2

Ce contre-exemple a été pris de [A-R-S].

Soit $A = M_3(k)$, où k est un corps de caractéristique 2, $G = \mathbb{Z}/2\mathbb{Z}$, qui agit sur A par conjugaison par la matrice

$$X := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

On vérifie que $X^2 = 1$, alors cette matrice définit bien une action de G. On peut faire le calcul explicite de cette action:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} . \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} . \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} a+c & b+c & c \\ d+f & e+f & f \\ a+d+g+c+f+i & b+e+h+c+f+i & c+f+i \end{pmatrix}$$

Si on appelle M la matrice générique précédente, on voit que $tr(M) = M + XMX =$

$$\begin{pmatrix} c & c & 0 \\ f & f & 0 \\ a+d+c+f+i & b+e+c+f+i & c+f \end{pmatrix}$$

ce qui montre que la trace d'aucun élément de $M_3(k)$ est égale à un.

En revanche, on peut se demander s'il existe des a_i et b_i. D'abord on remarque que

$$M_3(k)^G = \left\{ \begin{pmatrix} a & b & 0 \\ a+i & b+i & 0 \\ g & h & i \end{pmatrix} \ : \ a, b, g, h, i \in k \right\}$$

Si on appelle

$$B_1 := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad B_1' := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad B_2 := \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad B_3 := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Il est clair que B_1, B_1', B_2, et B_3 engendrent $A = M_3(k)$ comme A^G-module à gauche. En fait, B_1' appartient au A^G-sous-module engendré par B_1, et donc si les a_i, b_i de la définition de Galois existent, on peut supposer que les b_i sont les B_i qu'on vient d'écrire.

Avec exactement les mêmes techniques que dans l'exemple précédent on arrive à avoir des équations pour les A_i, sauf que dans ce cas il n'y a pas d'unicité. Mais quand même, on peut vérifier que, par exemple en choisisant

$$A_1 := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad A_2 := \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad A_3 := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

on a $A_1.B_1 + A_2.B_2 + A_3.B_3 = 1$ et $A_1.X.B_1.X + A_2.X.B_2.X + A_3.X.B_3.X = 0$.

Ce contre-exemple montre que la surjectivité de Tr n'est pas une conséquence de la surjectivité de β, et que l'énoncé non commutatif analogue au théorème 3.3 est faux. Un enoncé vrai, qui généralise celui du théorème 3.3 n'est pas évident.

6 Séparabilité

Le point de vue adopté par Ingraham et Demeyer dans [D-I] était celui de généraliser, pour les anneaux commutatifs, la notion de séparabilité et normalité, et alors définir une extension Galois comme une extension "normale et séparable".

Dans le cas non commutatif, la notion de séparabilité est plus ou moins claire, mais la notion de normalité (avec laquelle on veut principalement obtenir $Aut_{A^G}(A) = G$) est encore moins claire, on verra un exemple de extension Galois avec un groupe d'automorphismes énorme.

On rappelle que si $f : R \to S$ est un morphisme d'anneaux commutatifs, on dit que S est R séparable si S est un $S \otimes_R S$-module projectif. On remarque que dans le cas non commutatif, si l'image de f n'est pas contenue dans le centre de S, alors $S \otimes_R S$ n'est pas (au moins de façon évidente) un anneau. Il y a tout de même des propriétés semblables à la "séparabilité" quand R n'est pas commutatif: (voir [A-R-S] et [C-Q].)

Proposition 6.1 *Soit $f : R \to S$ un morphisme d'anneaux, les conditions suivantes sont équivalentes:*

1. *La multiplication $S \otimes_R S \to S$ admet une section qui est S-linéaire à gauche et à droite simultanément.*
2. *Pour tout S-module à gauche N, il existe une section naturelle (par rapport à N) du morphisme de structure $S \otimes_R N \to N$.*
3. *Pour tout S-bimodule M, si $D : S \to N$ est une dérivation qui s'annule sur R, alors D est intérieure.*

Esquisse de preuve

$1 \Rightarrow 2$. Soit $s : S \to S \otimes_R S$ un morphisme de S-bimodules qui scinde la multiplication. On dénote $s(1) = \sum_i a_i \otimes b_i$, et l'on a que pour tout $x \in S$, $s(x) = xs(1) = s(1)x$. D'après cette propriété, si l'on définit, pour un S-module à gauche N:

$$s_N : N \to S \otimes_R N$$

$$n \mapsto \sum_i a_i \otimes b_i n$$

est une section du morphisme de structure qui est S-linéaire, et naturelle par rapport à N.

$2 \Rightarrow 1$. Il faut prendre $N = {}_S S$ comme S-module à gauche. La naturalité par rapport aux morphismes de multiplication à droite implique la linéarité des deux côtés.

$1 \Rightarrow 3$. On garde les notations $s(1) = \sum_i a_i \otimes b_i$ qui vérifient $\sum_i a_i b_i = 1$ et $\sum_i x a_i \otimes b_i = \sum_i a_i \otimes b_i x$ pour tout $x \in S$.

On utilise la construction du $\Omega_R^{nc}(S) := Ker(m : S \otimes_R S \to S)$, le bimodule de 'différentiels non commutatifs'.

Ce bimodule a la propriété universelle suivante:

L'application $d : S \to \Omega_R^{nc}(S)$ définie par $d(s) = 1 \otimes s - s \otimes 1$ est une dérivation qui s'annule sur R. Et si M un S-bimodule et $D : S \to M$ une dérivation qui est nulle sur R, alors il existe un unique morphisme de bimodules $\widetilde{D} : \Omega_R^{nc}(S) \to M$ tel que $D = \widetilde{D} \circ d$, c'est-à-dire:

$$d^* : Hom_{S\ bimod}(\Omega_R^{nc}(S), M) \cong Der_R(S, M)$$

pour tout bimodule M.

Soit maintenant $x \in S$, $D : S \to M$ une dérivation qui s'annule sur R, $\widetilde{D} : \Omega_R^{nc}(S) \to M$ le morphisme de S-bimodules correspondant.

Grâce aux propriétés des a_i et b_i on a que, pour tout $x \in S$, $\sum_i x a_i \otimes b_i = \sum_i a_i \otimes b_i x$, et trivialement

$$\sum_i x a_i \otimes b_i - x \otimes 1 = \sum_i a_i \otimes b_i x - x \otimes 1$$

Mais l'avantage de la dernière égalité est qu'elle est une égalité dans $\Omega_R^{nc}(S)$. On applique $\widetilde{D}$ aux deux termes et l'on obtient

$$\sum_i xa_iD(b_i) - xD(1) = \sum_i a_iD(b_ix) - xD(1)$$

En utilisant le fait que D est une dérivation on obtient:

$$\sum_i xa_iD(b_i) = \sum_i a_iD(b_i)x + (\sum_i a_ib_i)D(x)$$

Comme $\sum_i a_ib_i = 1$, si on appelle $m_D := \sum_i a_iD(b_i)$, la formule précédente devient

$$D(x) = x.m_D - m_D.x = [x, m_D]$$

$3 \Rightarrow 1$.

La dérivation universelle $d : S \to \Omega_R^{nc}(S)$ définie par $d(x) = 1 \otimes x - x \otimes 1$ est nulle sur R, et donc par hypothèse elle est intérieure. Il existe alors $w \in \Omega_R^{nc}(S)$ tel que $d(x) = xw - wx$. On a l'égalité

$$1 \otimes x - x \otimes 1 = xw - wx$$

qui est valable pour tout $x \in S$. On dénote $e := (1 \otimes 1) + w$, alors $m(e) = 1$, et l'équation précédente est équivalente à $xe = ex$. Une section S-linéaire à droite et à gauche de la multiplication est donnée par exemple par $s(x) := x.e$.

Exemple: Soit (A, G) Galois, alors l'application $A \to A \otimes_{A^G} A$ définie par $x \mapsto \sum_i xa_i \otimes b_i = \sum_i a_i \otimes b_i x$ est une section A-linéaire à droite et à gauche.

On obtient plusieurs corollaires:

6.1 Dérivations

Corollaire 6.2 *Soit A un anneau commutatif, M un A-module symétrique, G un groupe fini d'automorphismes de A tel que A est une extension Galois de A^G. Alors toute dérivation A^G-linéaire $D : A \to M$ est nulle.*

Concernant la surjectivité, on utilise la proposition suivante pour les R-algèbres séparable:

Proposition 6.3 *Soit R un anneau commutatif, S une R-algèbre R-projective qui en plus est R-séparable. Si M est un S-module R-symétrique, et $d : R \to M$ une dérivation, alors il existe $D : S \to M$ tel que $D|_R = d$.*

Preuve: Soit $B = S \oplus M$ que l'on considère comme un anneau avec multiplication

$$(s, m)(s', m') := (ss', sm' + ms')$$

Comme $M^2 = 0$ et $d : R \to M$ est une dérivation, alors le morphisme $\phi : R \to B$ défini par $\phi(r) = (r, d(r))$ est un morphisme d'anneaux, et via ϕ, B est une R-algèbre. La projection

$$\pi : B \to S$$

$$(s, m) \mapsto s$$

est un morphisme de R-algèbres, avec noyau M. Comme les extensions de noyau M de carré nul de la R-algèbre S sont classifiées par $H_R^2(S, M) = Ext^2_{S \otimes_R S^{op}}(S, M)$, et S est supposé $S \otimes_R S^{op}$-projectif, alors $H_R^2(S, M) = 0$ et l'extension de R-algèbres qu'on vient de définir est triviale. Cela veut dire que la projection $B \to S$ admet une section $f : S \to B$ où f est un morphisme de R-algèbres.

Comme f est une section de la projection, $f(s)$ s'écrit nécessairement sous la forme $f(s) = (s, D(s))$, et le fait que f soit multiplicatif implique que $D : S \to M$ est une dérivation. Mais de plus, comme f est un morphisme de R-algèbres, alors $f|_R = \phi$, c'est-à-dire, pour tout $r \in R$, $f(r) = (r, D(r)) = \phi(r) = (r, d(r))$. Autrement dit, $D|_R = d$.

Corollaire 6.4 *Soit A un anneau commutatif, G un groupe fini d'automorphismes de A, et supposons que A est une extension Galois de A^G. Alors la restriction donne un isomorphisme $Der(A)^G \cong Der(A^G)$.*

6.2 Opérateurs différentiels

On a l'application évidente aux opérateurs différentielles:

Théorème 6.5 *Soit A un anneau intègre et régulier, $\mathbb{Q} \subseteq A$, G un groupe fini d'automorphismes de A, et supposons que A est une extension Galois de A^G. Alors Diff$(A^G) =$ Diff$(A)^G$.*

Preuve: Il existe toujours un morphisme de restriction $\mathrm{Diff}(A)^G \to \mathrm{Diff}(A^G)$, on verra qu'il est injectif et surjectif.

Comme A est régulier et l'on est en caractéristique zéro, Diff(A) est simple, ce qui implique que Diff$(A) * G$ est simple, et par invariance Morita Diff$(A)^G$ est simple aussi, alors la restriction est injective.

L'image de ce morphisme contient A^G et les restrictions de $Der(A)^G$, mais on sait que $\{D|_{A^G} : D \in Der(A)^G\} = Der(A^G)$, alors l'image contient A^G et $Der(A^G)$. On sait de plus que comme A est régulier, sous la condition Galois A^G est aussi régulier, ce qui implique que Diff(A^G) est engendrée comme algèbre par A^G et $Der(A^G)$, et donc le morphisme est surjectif.

Le résultat de localisation 1.4 fait que le corollaire suivant soit intéressant:

Corollaire 6.6 *Soit A un anneau commutatif intègre, G un sous-groupe fini des automorphismes de A. Soit $f \in A^G$ tel que $(A[f^{-1}], G)$ est Galois, alors la flèche naturelle Diff$(A)^G \to$ Diff(A^G) est injective, et son CoKer est un A^G-module de f-torsion.*

Preuve: elle est une conséquence immédiate du théorème précédent et du fait que la localisation des opérateurs différentiels s'identifie aux opérateurs différentiels de l'anneau localisé. On remarque que comme A est intègre régulière, Diff(A) est A-projectif (à gauche, ou à droite), donc sans torsion.

7 Homologie de Hochschild, homologie de De Rham

Dans cette section on calcule des invariants homologiques pour extensions de Galois commutatives (et presque commutatives).

Théorème 7.1 *(Théorème principal de [Lo]) Soit B un anneau commutatif qui contient $\mathbb{Q}$, et G un sous-groupe fini d'automorphismes de B tel que B est une extension Galois de B^G. Alors*

$$HH_*(B^G) = HH_*(B)_G$$

$$HH^*(B^G) = HH^*(B)^G$$

pour tout anneau de base $k \subset A^G$.

Comme B est une extension Galois de B^G alors $HH_*(B^G) = HH_*(B * G)$ et $HH^*(B^G) = HH^*(B * G)$. Pour calculer l'homologie et la cohomologie d'un produit croisé on a une suite spectrale, qui en caractéristique nulle dégénère dans un isomorphisme:

$$HH_*(B * G) = \oplus_{<g> \in <G>} H_*(B, B.g)_{\mathcal{Z}_g}$$

$$HH_*(B * G) = \oplus_{<g> \in <G>} H^*(B, B.g)^{\mathcal{Z}_g}$$

où $\mathcal{Z}_g$ est centralisateur de g dans G. La preuve du théorème sera achevée dès que l'on aura montré que les termes de cette somme correspondant aux $g \neq 1$ sont tous nuls.

Le lemme fondamental est le suivant:

Lemme 7.2 *Soit B une k-algèbre commutative, g un automorphisme de k-algèbres de B tel qu'il existe des éléments a_i, b_i dans B ($i \in I$ un ensemble fini) avec $\sum_{i \in I} a_i b_i = 1$ et $\sum_{i \in I} a_i g(b_i) = 0$. Alors $H_n(B, B.b) = 0 = H^n(B, B.g)$ pour tout n.*

Preuve: On montrera une homotopie de contraction dans le complexe standard. Le calcul homologique est complétement analogue au calcul cohomologique, on fera les calculs explicites dans le cas homologique.

Rappelons que l'homologie de B à coefficients dans $B.g$ est l'homologie du complexe

$$\ldots \to B.g \otimes B^{\otimes n} \to \ldots \to B.g \otimes B \to B.g \to 0$$

avec la différentielle donnée par

$$b(ag, c_1, \ldots, c_n) = (ag(c_1), c_2, \ldots, c_n) +$$

$$+ \sum_{i=1}^{n-1} (-1)^i (ag, c_1, \ldots, c_i c_{i+1}, \ldots, c_n) + (-1)^n (c_n ag, c_1, \ldots, c_{n-1})$$

On définit l'homotopie

$$s : Bg \otimes B^{\otimes n} \to Bg \otimes B^{\otimes n+1}$$

$$s(ag, c_1, \ldots, c_n) := \sum_{i \in I, k=1}^{n+1} (-1)^k (a_i ag, c_1, \ldots, c_{k-1}, b_i, c_k, \ldots, c_n)$$

(dans cette notation, le premier terme est $(a_i ag, b_i, c_1, \ldots, c_n)$ et le terme $n+1$ est $(a_i ag, c_1, \ldots, c_n, b_i)$.)

On se contentera ici de faire le calcul dans les petits degrés:
À un élément ag dans Bg correspond l'élément

$$\sum_{i \in I} (-1)(a_i ag, b_i) \longmapsto - \sum_{i \in I} a_i ag(b_i) + \sum_{i \in I} b_i a_i ag = ag$$

Le calcul en général est sans malice.

Remarques:

1. Le A-module $H_0(A, Ag)$ se calcule de la façon suivante en termes de l'idéal I_g: $Ag/[A, Ag] = (A/[A, A]_g).g = (A/\{ab - bg(a) \ : \ a, b \in A\}).g = (A/I_g).g$. De plus, c'est un A-module cyclique engendré par la classe de 1, alors dans le cas où il n'est pas nul, il existe au moins un élément non nul G-invariant. On voit donc que si A est une algèbre (commutative) et G un groupe fini d'automorphismes tel que le morphisme naturel $HH_*(A)^G \to HH_*(A * G)$ est un isomorphisme, en particulier $H_0(A, Ag)^{\mathcal{Z}_g} = 0$ pour les $g \neq 1$, ce qui entraîne $I_g = A$ pour tout $g \neq 1$, c'est-à-dire que l'action est Galois. On peut caractériser les extensions de Galois (commutatives) par la propriété suivante: étant donnée A commutative, alors (A, G) Galois si et seulement si $HH_*(A)^G = HH_*(A * G)$.

2. Si M est un B-bimodule, on dit que M est g-central si et seulement si $m.b = g(b).m$ pour tout $b \in B$, $m \in M$. Si M est un tel bimodule, le lemme reste valable (avec le même calcul) si on remplace $HH_*(B, B.g)$ par $HH_*(B, M)$ et $HH^*(B, B.g)$ par $HH^*(B, M)$.

3. La preuve du théorème 7.1 est finie.

Comme conséquence immédiate, en regardant $HH^1(A^G)$ on retrouve que $Der_k(A^G) = Der_k(A)^G$. De plus (avec le HH_1) $\Omega^1_k(A^G) = \Omega^1_k(A)_G$.

Pour les extensions d'anneaux intègres en général (i.e. non nécessairement de Galois) on a le résultat suivant:

Corollaire 7.3 *Soit A un anneau commutatif intègre, G un sous-groupe fini d'automorphismes de A. Alors la flèche*

$$HH_n(A^G) \to HH_n(A)^G$$

a pour noyau et conoyau des A^G-modules de f-torsion, pour tout $f \in A^G$ tel que $A[f^{-1}]$ soit une extension de Galois de $A^G[f^{-1}]$.

Preuve: On utilise le théorème précédent pour $A[f^{-1}]$ et le fait que que la localisation soit un foncteur exact et commute avec l'homologie de Hochschild.

Un argument de suites spectrales donne la généralisation suivante aux algèbres quasi-commutatives:

Théorème 7.4 *Soit C une k-algèbre commutative avec $\mathbb{Q} \subseteq k$, on suppose la filtration positive et exhaustive, et G un sous-groupe fini d'automorphismes (k-linéaires) préservant la filtration. Si $gr(C)$ est commutatif et $gr(C)$ est une extension Galois de $gr(C)^G$, alors $HH_*(C^G) = HH_*(C)_G$.*

Corollaire 7.5 *Soit A une k-algèbre commutative lisse intègre qui contient $\mathbb{Q}$ et G un sous-groupe fini d'automorphismes de A. On suppose que A est une extension Galois de A^G, alors $H^*_{dR}(A^G) = H^*_{dR}(A)_G$.*

Preuve: Comme A est lisse, la condition de Galois nous dit que A^G est lisse aussi. Par le théorème Wodzicki-Brylinski (voir [Wo] ou [Br]) $H^*_{dR}(A^G) = HH_{2d-*}(\mathrm{Diff}(A^G))$. Mais sous ces hypothèses, $\mathrm{Diff}(A^G) = \mathrm{Diff}(A)^G$, et comme A est lisse $\mathrm{Diff}(A)^G$ est toujours Morita équivalent à $\mathrm{Diff}(A) * G$, ce qui prouve $HH_{2d-*}(\mathrm{Diff}(A^G)) = HH_{2d-*}(\mathrm{Diff}(A)^G) = HH_{2d-*}(\mathrm{Diff}(A) * G)$. On peut donc utiliser le théorème précédent pour $C = \mathrm{Diff}(A)$; Dans ce cas, $gr(\mathrm{Diff}(A))_0 = A$ est une extension Galois de A^G, alors $HH_{2d-*}(\mathrm{Diff}(A) * G) = HH_{2d-*}(\mathrm{Diff}(A))_G$. On utilise une autre fois le résultat de Wodzicki-Brylinski dans le sens inverse et l'on obtient $HH_{2d-*}(\mathrm{Diff}(A))_G = H^*_{dR}(A)_G$.

Références

[Le] T. Levasseur: Anneaux d'opérateurs différentiels. L.N.Math. Springer 867 (1981), 157-173.

[A-F] F. Anderson - K.Fuller: Rings and categories of modules. 2. ed. Graduate Texts in Mathematics. 13. New York: Springer-Verlag.

[C-Q] J.Cuntz, D. Quillen: Cyclic homology and nonsingularity. J. Am. Math. Soc. 8, No.2, 373-442 (1995).

[A-R-S] M. Auslander, I. Reiten, S. Smalo: Galois actions on rings and finite Galois coverings. Math. Scand. 65, No.1, 5-32 (1989).

[C-F-M] M.Cohen, D.Fischman, S. Montgomery: Hopf Galois extensions, smash products, and Morita equivalence. J. Algebra 133, No.2, 351-372 (1990).

Voir aussi: M.Cohen: A Morita context related to finite automorphism groups of rings. Pac. J. Math. 98, 37-54 (1982).

[K-T] H. Kreimer, M. Takeuchi: Hopf algebras and Galois extensions of an algebra. Indiana Univ. Math. J. 30, 675-692 (1981).

[Lo] M. Lorenz: On Galois descent for Hochschild and cyclic homology. Comment. Math. Helv. 69 (1994), no. 3, 474-482 (1994).

[Mo] S. Montgomery: Fixed rings of finite automorphism groups of associative rings. Lecture Notes in Mathematics, 818. Berlin - Heidelberg - New York: Springer-Verlag.

[C-H-R] S. Chase, D.Harrison, A. Rosenberg: Galois theory and Galois cohomology of commutative rings. Mem. Am. Math. Soc. 52, 15-33 (1965).

[D-I] F. Demeyer, E. Ingraham: Separable algebras over commutative rings Berlin - Heidelberg - New York: Springer-Verlag, 157 p. (1971).

[Fe] M. Ferraro: On the Galois theory of non-commutative rings. Osaka J. Math. 7, 81-88 (1970).

[Wo] M. Wodzicki: Cyclic homology of differential operators. Duke Math. J. 54, 641-647 (1987).

[Br] J.L.Brylinski: A differential complex for Poisson manifolds. J. Differ. Geom. 28, No.1, 93-114 (1988).