Révision introductive

De la théorie de Galois sur les anneaux commutatifs

Lionel Ducos

Année 2003 (recompilé le 6 juillet 2011)

Table des matières

Abstract

In this paper, the concept of a galois algebra is introduced by linear algebraic methods, an aspect perhaps too often left a side in the literature.

In the first part, we approach classical results in different way, a particular point is put on the intrinsic aspect of the formulas obtained. We will also see that the idempotents elements play a significant role in the theory of endomorphisms and automorphisms of the galois algebras.

A study of groups of homomorphisms will allow us to obtain a unusual one-to-one correspondence but simple (implying in a trivial way the traditional correspondence within fields), not using the assumption relating the idempotents elements, contrary to [DI] (with

no idempotents except 0 and 1), [CHR], [FP] (with strongly distinct homomorphisms), or [VZ] (with finitely many idempotents).

Lastly, a small application of this unusual one-to-one correspondence will deal with the generating systems of invariant subalgebras.

Résumé

Dans ce document, la notion d'algèbre galoisienne est introduite par le biais de l'algèbre linéaire, un aspect peut-être trop souvent laissé de côté dans la littérature.

Dans les énoncés des résultats (tout à fait classiques) de la première partie, un point particulier est mis sur l'aspect intrinsèque (ou pas) des formules obtenues. Nous verrons également que les idempotents jouent un rôle important dans la connaissance des endomorphismes et automorphismes des algèbres galoisiennes.

L'étude de certains groupes d'homomorphismes permettra d'obtenir une correspondance galoisienne inhabituelle mais simple (impliquant trivialement la correspondance classique dans le cadre des corps), ne faisant pas intervenir d'hypothèse concernant les idempotents, contrairement à [DI], [CHR], [FP] ou [VZ].

Enfin, une petite application de cette correspondance galoisienne inhabituelle portera sur les systèmes générateurs de sous-algèbres invariantes.

1 Brefs rappels sur les modules projectifs

Définition 1.1 ([Bou2], p.61) *Soit M un R-module. On dit que M est **projectif** si M est isomorphe à un facteur direct d'un R-module libre.*

Propriété 1.2 ([Bou2], p.70-71) *Soit M un R-module et $(a_t)_{t\in T}$ un système générateur quelconque de M. Il y a équivalence entre les assertions suivantes :*

- *M est un R-module projectif ;*
- *il existe une famille $(a_t^*)_{t\in T}$ de formes linéaires sur M telles que, pour tout $x \in M$, la famille $(a_t^*(x))_{t\in T}$ ait un support fini et que l'on ait*

$$x = \sum_{t\in T} a_t^*(x)a_t$$

On dit que les familles $(a_t)_{t\in T}$ et $(a_t^*)_{t\in T}$ forment un système de coordonnées.
Si T est une famille finie, alors on peut définir la matrice P (à coefficients dans R) par $P_{i,j} = a_j^*(a_i)$ pout $i, j \in T$. On vérifie facilement que $P^2 = P$, donc que P est une **matrice de projection** :

$$P_{i,j}^2 = \sum_{k\in T} P_{i,k}P_{k,j} = \sum_{k\in T} a_k^*(a_i)a_j^*(a_k) = a_j^*\left(\sum_{k\in T} a_k^*(a_i)a_k\right) = a_j^*(a_i) = P_{i,j}$$

Propriété 1.3 ([Bou2], p.110-112) *Soit M un R-module et $M^* = L_R(M,R)$ le dual de M. Si M est projectif de type fini, alors les deux homomorphismes canoniques suivants sont bijectifs :*

$$\begin{array}{rcl} M^* \otimes_R M & \longrightarrow & L_R(M,M) = \mathrm{End}_R(M) \\ a^* \otimes m & \longmapsto & (x \mapsto a^*(x)m) \end{array}$$

$$\begin{array}{rcl} M \otimes_R M & \longrightarrow & L_R(M^*,M) \\ x \otimes m & \longmapsto & (a^* \mapsto a^*(x)m) \end{array}$$

Définition 1.4 ([Bou2], p.112) *Soit R un anneau commutatif, M un R-module, et M^* son dual. On définit la **trace** d'un élément de $M^* \otimes_R M$ par $\mathrm{tr}(a^* \otimes m) = a^*(m)$.*

Par suite, si M est projectif de type fini, on peut transporter cette trace canonique sur $L_R(M,M) \simeq M^* \otimes_R M$.

Dans le cas où M est libre sur R, il s'agit de la trace usuelle sur $L_R(M,M)$.

Explicitons la trace de $u \in \mathrm{End}_R(M)$: l'application $\mathrm{Id} \in \mathrm{End}_R(M)$ est l'image d'un élément de $M^* \otimes_R M$, c'est-à-dire qu'il existe deux familles finies $(a_t)_{t\in T}$ de M et $(a_t^*)_{t\in T}$ de formes linéaires sur M telles que :

$$\forall\ x \in M, \quad x = \sum_{t\in T} a_t^*(x) a_t$$

Ainsi, on a $u(x) = \sum_t a_t^*(x) u(a_t)$, donc l'image de u dans $M^* \otimes_R M$ est $\sum_t a_t^* \otimes u(a_t)$. On a donc

$$\mathrm{tr}(u) = \sum_{t\in T} a_t^*(u(a_t))$$

Cette égalité est **indépendante** du choix des familles $(a_t)_{t\in T}$ et $(a_t^*)_{t\in T}$.

Dans le cas où M est de plus un anneau, on définit également la **forme bilinéaire tracique** par

$$\begin{array}{rcl} M \times M & \longrightarrow & R \\ (x,y) & \longmapsto & \mathrm{tr}(xy) \end{array}$$

et le **discriminant** d'une famille finie $(v_i)_i$ par $\det\big(\mathrm{tr}(v_i v_j)\big)_{i,j}$. En particulier, la forme bilinéaire tracique donne naissance à une application R-linéaire de M dans son dual M^* :

$$\begin{array}{rcl} M & \longrightarrow & M^* \\ x & \longmapsto & \mathrm{tr}(x\cdot) : y \mapsto \mathrm{tr}(xy) \end{array}$$

Soit R un anneau commutatif et A un sur-anneau entier sur R. Supposons que A soit projectif. Alors A est un anneau **fidèlement plat** sur R : tout module projectif est plat (voir [Bou1], p.28), et le fait d'être entier le rend fidèlement plat (voir [Bou1], p.51) en se servant du relèvement des idéaux premiers et maximaux (voir [Bou3]). Deux propriétés essentielles des modules (fidèlement) plats sont les suivantes :

Propriété 1.5 ([Bou1], p.26) *Soit A un R-module plat et $N' \to N \to N''$ une suite exacte de R-modules. Alors $N' \otimes_R A \to N \otimes_R A \to N'' \otimes_R A$ est exacte.*

En particulier, les injections ($N' = (0)$) et les surjections ($N'' = (0)$) sont conservées via la tensorisation par A.

Propriété 1.6 ([Bou1], p.44) *Si A est un R-module fidèlement plat, alors une suite $N' \to N \to N''$ est exacte si et seulement si $N' \otimes_R A \to N \otimes_R A \to N'' \otimes_R A$ est exacte.*

2 Approche linéaire des algèbres galoisiennes

Proposition 2.1 *Soit A un anneau commutatif unitaire, R un sous-anneau de A, G sous-groupe fini de $\mathrm{Aut}_R(A)$. Si A est un R-module projectif de type fini et G une A-base de $L_R(A, A)$, alors*

- *$R = A^G$;*
- *A est un R-module fidèlement plat ;*
- *$\forall\ x \in A$, on a $\mathrm{tr}(x) = \sum_{g \in G} g(x)$ (écriture indépendante de G) ;*
- *la forme linéaire trace est dualisante, i.e. l'application $\left\{ \begin{array}{ccc} A & \longrightarrow & A^* \\ a & \longmapsto & \mathrm{tr}(a\cdot) \end{array} \right.$ est un isomorphisme R-linéaire, en particulier l'application bilinéaire tracique est non dégénérée, i.e. $(\forall\ x \in A,\ \mathrm{tr}(ax) = 0) \Rightarrow a = 0$.*
- *pour toute famille génératrice finie $(a_t)_{t \in T}$ de A sur R, il existe une famille $(b_t)_{t \in T}$ de A, génératrice, finie, indépendantes de G, telle que*

$$\forall\ x \in A, \quad x = \sum_{t \in T} \mathrm{tr}(a_t x) b_t = \sum_{t \in T} \mathrm{tr}(b_t x) a_t$$

$$\forall\ g, g' \in G, \quad \sum_{t \in T} g(b_t) g'(a_t) = \delta_{g,g'}$$

- *en posant $P_a = \big(g(a_j)\big)_{\substack{g \in G \\ j \in T}}$, $P_b = \big(g(b_j)\big)_{\substack{g \in G \\ j \in T}}$, $M_y = \big(\mathrm{tr}(a_i b_j y)\big)_{\substack{i \in T \\ j \in T}}$ (la matrice de la multiplication par y dans le système de coordonnées $(a_t)_t$, $(b_t)_t$) et D_y la matrice diagonale formée par $\big(g(y)\big)_{g \in G}$ pour $y \in A$, on a :*

$$P_a . {}^t P_b = \mathrm{Id}_{|G|} = P_b . {}^t P_a \quad , \quad M_y = {}^t P_a . D_y . P_b \quad , \quad D_y = P_b . M_y . {}^t P_a$$

- *on dispose d'isomorphimes A-linéaires canoniques :*

$$\begin{array}{ccccc} A \otimes_R A & \widetilde{\longrightarrow} & A^* \otimes_R A & \widetilde{\longrightarrow} & L_R(A, A) \\ b \otimes a & \longmapsto & \mathrm{tr}(b\cdot) \otimes a & \longmapsto & \mathrm{tr}(b\cdot)a \\ \sum_t b_t \otimes f(a_t) & \longmapsto & \sum_t \mathrm{tr}(b_t \cdot) \otimes f(a_t) & \longmapsto & f \end{array}$$

– *de la forme bilinéaire tracique $A^2 \to R$, on déduit une forme A-bilinéaire symétrique sur $L_R(A,A)$*

$$\langle w, v\rangle = \sum_{t\in T} w(a_t)v(b_t) \quad \textit{(indépendant des } (a_t)_t, (b_t)_t \textit{ et } G\textit{)}$$

dont G forme une A-base orthonormale.

Démonstration On suppose que l'anneau A (contenant R) est un R-module **projectif de type fini**. Considérons $(a_t)_t \subset A$ et $(a_t^*)_t \subset A^*$ un système fini de coordonnées de A sur R.

Comme A est un anneau (commutatif), on peut définir la **trace d'un élément** $x \in A$ comme étant la trace de l'endomorphisme de multiplication par x, que l'on peut écrire (de manière indépendante du choix des $(a_t)_t$ et $(a_t^*)_t$) :

$$\mathrm{tr}(x) = \sum_{t\in T} a_t^*(xa_t)$$

Du fait que A soit un anneau entier sur R (car de type fini), la somme I des idéaux $(a_t^*(A))_t \subset R$ ne peut pas être propre (car $A = I.A$), donc $1 \in I$, c'est-à-dire qu'il existe $(c_t)_t \subset A$ tel que $1 = \sum_t a_t^*(c_t)$.

Autre conséquence que A soit un anneau, le groupe des applications R-linéaires $L_R(A,A)$ est muni d'une structure de A-module, en posant $(a.f)(x) = af(x)$. Ce A-module n'a aucune raison d'être libre, mais supposons qu'il existe G un sous-groupe fini des **R-automorphismes de** A formant une **A-base de** $L_R(A,A)$.

Remarque. Si A est libre sur R, alors son rang est égal au cardinal de G :

$$[A : R] = [L_R(A,R) : R] = [L_R(A,A) : A] = |G|$$

Alors les applications R-linéaires de $L_R(A,A)$ sont A^G-linéaires. (A^G est le sous-anneau de A formé par les points invariants sous l'action de G.) Ainsi, pour tout $x \in A^G$, on a $x = \sum_t a_t^*(c_t)x = \sum_t a_t^*(c_t x) \in R$, c'est-à-dire $A^G \subset R$. L'inclusion inverse est évidente...

Remarque. L'égalité $R = A^G$ confirme d'une autre manière que A est entier R : tout élément $x \in A$ est racine de $\prod_{y\in G.x}(T-y)$ à coefficients dans R (résolvante de x). Comme A est projectif sur R, il est donc fidèlement plat.

Comme G est une A-base de $L_R(A,A) \supset L_R(A,R)$, quel que soit $h \in L_R(A,R)$, on peut écrire de manière unique $h = \sum_g h_g g$ avec $h_g \in A$. Or $f \circ h = h$ (car h est à valeurs dans R) pour tout $f \in G$, donc

$$\sum_{g\in G} f(h_g) fg = f \circ h = h = \sum_{g\in G} h_g g = \sum_{g\in G} h_{fg} fg$$

D'où $f(h_g) = h_{fg}$, et en posant, $g = \mathrm{Id}$ on obtient $f(h_{\mathrm{Id}}) = h_f$ pour tout $f \in G$. Conclusion :

$$(\star) \quad \forall\ h \in A^*, \exists!\ b \in A, \quad h = \sum_{f \in G} f(b) f$$

En particulier, pour tout $t \in T$, posons $a_t^* = \sum_g g(b_t) g$. Comme A est projectif de type fini, on a $x = \sum_t a_t^*(x) a_t$, d'où pour tout $g' \in G$

$$g'(x) = \sum_{t \in T} a_t^*(x) g'(a_t) = \sum_{t \in T} \sum_{g \in G} g(b_t) g(x) g'(a_t) = \sum_{g \in G} \left(\sum_{t \in T} g(b_t) g'(a_t) \right) g(x)$$

Or G est une famille libre sur A, on obtient donc :

$$(\star\star) \qquad \forall\ g, g' \in G, \quad \sum_{t \in T} g(b_t) g'(a_t) = \delta_{g,g'} \quad \text{(symbole de Kronecker)}$$

En particulier, $\sum_t b_t a_t = 1$, et, enfin, un calcul rassurant :

$$\mathrm{tr}(x) = \sum_{t \in T} a_t^*(x a_t) = \sum_{t \in T} \sum_{g \in G} g(b_t a_t x) = \sum_{g \in G} g \left(\sum_{t \in T} b_t a_t \right) g(x) = \sum_{g \in G} g(x)$$

Remarquons, maintenant que l'on sait que $\sum_{g \in G} g(x) = \mathrm{tr}(x)$ ne dépend pas des éléments de G, que l'isomorphisme entre A et A^* donné par $(\star)$ ne dépend pas de G : $\forall\ h \in A^*, \exists!\ b \in A, \quad h = \mathrm{tr}(b\cdot)$.

Posons $P_a = \big(g(a_j)\big)_{\substack{g \in G \\ j \in T}}$, $P_b = \big(g(b_j)\big)_{\substack{g \in G \\ j \in T}}$, $M_y = \big(\mathrm{tr}(a_i b_j y)\big)_{\substack{i \in T \\ j \in T}}$ et D_y la matrice diagonale formée par $\big(g(y)\big)_{g \in G}$ pour $y \in A$. La relation $(\star\star)$ est synonyme de $P_a . {}^t P_b = \mathrm{Id}_{|G|} = P_b . {}^t P_a$. On vérifie facilement $M_y = {}^t P_a . D_y . P_b$: si $i, j \in T$ alors

$$\big({}^t P_a . D_y . P_b\big)_{i,j} = \sum_{g, g' \in G} g(a_i) \delta_{g,g'} g'(y) g'(b_j) = \sum_{g \in G} g(a_i b_j y) = (M_y)_{i,j}$$

on obtient $P_b . M_y . {}^t P_a = P_b . {}^t P_a . D_y . P_b . {}^t P_a = D_y$.

Remarque. Avec $D_y = P_b . M_y . {}^t P_a$ pour tout $y \in A$, on commence à voir que $A \otimes_R A$ s'injecte dans $A^{|G|} = \prod_G A$.

D'autre part, la formule $(\star\star)$ est visiblement symétrique en les $(a_t)_t$ et $(b_t)_t$. Le lecteur pourra vérifier facilement (en remontant les calculs) que toutes les propriétés établies avec les $(a_t)_t, (b_t)_t$ peuvent l'être également avec les $(b_t)_t, (a_t)_t$, notamment

$$\forall\ x \in A, \quad x = \sum_{t \in T} \mathrm{tr}(a_t x) b_t = \sum_{t \in T} \mathrm{tr}(b_t x) a_t$$

Exemple 2.2 Prenons un exemple extrêmement simple en posant $A = R^n$ et G un sous-groupe de $\mathcal{S}_n$, d'ordre n et transitif sur $[1, n]$. L'opération de G sur A consiste à permuter les coordonnées.

Il est clair que pour $n \geqslant 4$, le groupe G n'est pas unique et on peut choisir de manière tout-à-fait indépendante de G les éléments a_t, à savoir les éléments de la base canonique. Les éléments b_t jouent un rôle tellement symétrique que l'on peut les prendre respectivement égaux aux a_t ! Quant à elle, la trace d'un élément de A est bien sûr la somme de ses coordonnées, ce qui est également indépendant du choix de G (transitif et d'ordre n)...

En utilisant la propriété 1.3 on obtient :

$$\begin{array}{ccccc} A \otimes_R A & \xrightarrow{\sim} & A^* \otimes_R A & \xrightarrow{\sim} & L_R(A,A) \\ b \otimes a & \longmapsto & \mathrm{tr}(b\cdot) \otimes a & \longmapsto & \mathrm{tr}(b\cdot)a \\ 1 \otimes 1 & \longmapsto & \mathrm{tr} \otimes 1 & \longmapsto & \mathrm{tr} \\ \sum_t b_t \otimes f(a_t) & \longmapsto & \sum_t \mathrm{tr}(b_t\cdot) \otimes f(a_t) & \longmapsto & f \end{array}$$

On peut prolonger la forme R-bilinéaire tracique $A^2 \to R$ en une forme A-bilinéaire symétrique $(A \otimes_R A)^2 \to A$ en posant $\langle a \otimes a', b \otimes b' \rangle = \mathrm{tr}(ab)a'b'$, puis via l'isomorphisme $A \otimes_R A \simeq L_R(A, A)$ ci-dessus, on en obtient une autre sur $L_R(A, A)$ donnée par $\langle \mathrm{tr}(a\cdot)a',\ \mathrm{tr}(b\cdot)b' \rangle = \mathrm{tr}(ab)a'b'$.

Explicitons concrètement cette forme A-bilinéaire symétrique pour deux éléments $w, v \in L_R(A, A)$. Écrivons :

$$\begin{array}{c} w = \sum_u \mathrm{tr}(a_u\cdot)w(b_u) = \sum_u \mathrm{tr}(b_u\cdot)w(a_u) \\ v = \sum_t \mathrm{tr}(a_t\cdot)v(b_t) = \sum_t \mathrm{tr}(b_t\cdot)v(a_t) \end{array}$$

Comme $\langle \mathrm{tr}(b_u\cdot)w(a_u),\ \mathrm{tr}(a_t\cdot)v(b_t) \rangle = \mathrm{tr}(b_u a_t)w(a_u)v(b_t) = w\big(\mathrm{tr}(b_u a_t)a_u\big)v(a_t)$ et $\sum_u \mathrm{tr}(b_u a_t)a_u = a_t$, on obtient par bilinéarité

$$\langle w, v \rangle = \sum_{t \in T} w(a_t)v(b_t)$$

Dans cette formule, les familles $(a_t)_t, (b_t)_t$ ont bien sûr des rôles symétriques, mais surtout cette forme A-bilinéaire symétrique définie sur $L_R(A, A)$ est canonique (ne dépend pas des $(a_t)_t, (b_t)_t$). Enfin, la formule $(\star\star)$ raconte exactement que G est une famille orthonormale pour cette formule bilinéaire. □

3 Idempotents et $\mathrm{Hom}_R(A, A)$

Proposition 3.1 *Soit A un anneau commutatif unitaire, R un sous-anneau de A, G sous-groupe fini de $\mathrm{Aut}_R(A)$. Si A est un R-module projectif de type fini et G une A-base de $L_R(A, A)$, alors*

– *pour tout $v, w \in L_R(A,A)$, on définit*

$$v * w = \sum_{g\in G} \langle v, g\rangle \langle w, g\rangle g \qquad \textit{(écriture indépendante de } G\textit{)}$$

et en particulier $(v * w)(1) = \langle v, w\rangle$;

– *$G \subset L_R(A,A)$ (muni de $*$) est un système fondamental d'idempotents orthogonaux non nuls. En particulier, $A \otimes_R A$ et $L_R(A,A)$ (muni de $*$) sont isomorphes à $\prod_G A$ en tant que A-algèbres (isomorphismes dépendant de G).*

$$\begin{array}{ccccc} A\otimes_R A & \xrightarrow{\sim} & L_R(A,A) & \xrightarrow{\sim} & \prod_G A \\ & & f & \longmapsto & \big(\langle f, g\rangle\big)_{g\in G} \\ b\otimes a & \longmapsto & \mathrm{tr}(b\cdot)a & \longmapsto & \big(g(b)a\big)_{g\in G} \end{array}$$

Démonstration Nous avons déjà établi quelques résultats, notamment un isomorphisme entre $A \otimes_R A$ et $L_R(A,A)$. Dans chacun de ces A-modules, certaines notions se définissent naturellement et n'ont *a priori* pas d'équivalent dans l'autre module. Par exemple, la multiplication interne de $A \otimes_R A$ ne correspond pas à la composition dans $L_R(A,A)$. De même, les notions de composition et de R-automorphisme (d'algèbre) dans $L_R(A,A)$ ne s'interprètent pas aisément dans $A \otimes_R A$.

Les algèbres $A \otimes_R A$ et $A^* \otimes_R A$ ont permis de définir de manière intrinsèque certaines notions (par exemple la trace et la forme bilinéaire tracique), mais l'ensemble $L_R(A,A)$ présente des qualités intéressantes pour les calculs.

À titre d'exemple, transférons l'action de G sur A dans $L_R(A,A)$, via $A\otimes_R A$: comme G opère sur A, on prolonge cette opération sur $A \otimes_R A$ par $g.(a \otimes b) = g(a) \otimes b$ (les scalaires sont $1 \otimes a$), puis sur $L_R(A,A)$ (via l'isomorphisme). En posant $L_R(A,A) \ni v = \sum_t \mathrm{tr}(b_t\cdot)v(a_t)$, on obtient

$$g.v = \sum_{t\in T} \mathrm{tr}(g(b_t)\cdot)v(a_t) = v\left(\sum_{t\in T} \mathrm{tr}(b_t g^{-1}(\cdot))a_t\right) = v \circ g^{-1}$$

Remarque. Cette opération serait la même si g était un R-automorphisme quelconque de A laissant la trace invariante : $\mathrm{tr}\circ g = \mathrm{tr}$.

L'opération de G sur A se transporte en l'opération de composition à droite par l'inverse dans $L_R(A,A)$. En particulier, le groupe G est une base normale de $L_R(A,A)$.

Nous décidons arbitrairement de transporter la multiplication de $A\otimes_R A$ sur $L_R(A,A)$, munissant ainsi de manière canonique $L_R(A,A)$ d'une structure de A-algèbre commutative : pour $v, w \in L_R(A,A)$, on a dans $A \otimes_R A$

$$\left(\sum_{t\in T} a_t \otimes v(b_t)\right) \times \left(\sum_{u\in T} b_u \otimes w(a_u)\right) = \sum_{t,u\in T} a_t b_u \otimes v(b_t)w(a_u)$$

ce qui se traduit dans $L_R(A,A)$ par

$$\begin{aligned} v*w &= \sum_{t,u\in T} \mathrm{tr}(a_t b_u \cdot) v(b_t) w(a_u) \\ &= \sum_{t,u\in T} \sum_{g\in G} g(a_t) g(b_u) g(\cdot) v(b_t) w(a_u) \\ &= \sum_{g\in G} \left(\sum_{t\in T} g(a_t) v(b_t) \right) \left(\sum_{u\in T} g(b_u) w(a_u) \right) g \\ v*w &= \sum_{g\in G} \langle v, g\rangle \langle w, g\rangle g \end{aligned}$$

et en particulier

$$(v*w)(1) = \sum_{t,u\in T} \mathrm{tr}(a_t b_u) v(b_t) w(a_u) = \langle v, w\rangle$$

On voit clairement que cette multiplication $*$ est en fait la multiplication de A composante à composante lorsque l'on écrit les éléments de $L_R(A,A)$ dans la base G. En particulier, on a $f*g = \langle f, g\rangle g$ pour $f \in L_R(A,A)$ et $g \in G$, si bien que les éléments de G sont des idempotents orthogonaux (pour $*$).

> Remarque. Bien sûr, on peut montrer que l'image d'un élément de G dans $A \otimes_R A$ est un "vrai" idempotent, mais cela demande un (petit) calcul astucieux utilisant l'isomorphisme entre $A \otimes_R A$ et $L_R(A,A)$. Alors autant travailler directement dans $L_R(A,A)$!

Une conséquence directe est que $L_R(A,A)$ (muni de $*$) est isomorphe à $\prod_G A$ en tant que A-algèbre :

$$\begin{array}{ccccc} A \otimes_R A & \xrightarrow{\sim} & L_R(A,A) & \xrightarrow{\sim} & \prod_G A \\ & & f & \longmapsto & \big(\langle f, g\rangle \big)_{g\in G} \\ b\otimes a & \longmapsto & \mathrm{tr}(b\cdot)a & \longmapsto & \big(g(b)a\big)_{g\in G} \\ 1\otimes 1 & \longmapsto & \mathrm{tr} & \longmapsto & 1 \end{array}$$

□

Propriété 3.2 *Avec les mêmes notations et hypothèses que la proposition 3.1, l'ensemble* $\mathrm{Hom}_R(A,A)$ *des endomorphismes de la R-algèbre A est en bijection avec les systèmes fondamentaux d'idempotents orthogonaux $(s_g)_{g\in G}$ de A (indépendamment de G), certains s_g pouvant être nuls, via $(s_g)_g \longmapsto \sum_g s_g.g$ (voir [CHR], p.25-26). En particulier,*

$$f \in \mathrm{Hom}_R(A,A) \quad \Longrightarrow \quad f*f = f \quad et \quad \langle f, f\rangle = 1$$

Démonstration Soit $f \in L_R(A,A)$, $g \in G$ et $a \in A$. En écrivant $f = \sum_g \langle f, g\rangle g$, on vérifie facilement que $\langle f(a\cdot), g(\cdot)\rangle = g(a)\langle f, g\rangle$. Si de plus f est application multiplicative, $f(ab) = f(a)f(b)$, alors $f(a)\langle f, g\rangle = g(a)\langle f, g\rangle$, et ceci pour tout $a \in A$, d'où $\langle f, g\rangle f = \langle f, g\rangle g$. Si $g' \in G$, alors

$$\langle f, g\rangle \langle f, g'\rangle = \langle \langle f, g\rangle f, g'\rangle = \langle \langle f, g\rangle g, g'\rangle = \langle f, g\rangle \delta_{g,g'}$$

Enfin, si $f \in \mathrm{Hom}_R(A,A)$ alors $1 = f(1) = \sum_{g\in G} \langle f, g\rangle$, si bien que $(\langle f, g\rangle)_{g\in G}$ est un système fondamental d'idempotents orthogonaux de A.

Réciproquement, si $(s_g)_{g\in G}$ est un s.f.i.o, alors on vérifie facilement que $\sum_g s_g g$ est une application linéaire multiplicative fixant 1.

Pour terminer, $f * f = f$ est impliqué par $\langle f, g\rangle^2 = \langle f, g\rangle$ pour tout $g \in G$, et $\langle f, f\rangle = 1$ par $\sum_g \langle f, g\rangle^2 = 1$. □

4 Définition et exemples élémentaires

Définition 4.1 *Soit un anneau commutatif A, R un sous-anneau de A, G un sous-groupe fini de $\mathrm{Aut}_R(A)$. La R-algèbre A est dite* ***galoisienne de groupe*** *G si elle vérifie l'une des assertions équivalentes suivantes :*

1. *A est un R-module projectif de type fini et G une A-base de $L_R(A,A)$;*
2. *[Len] : A est un R-module projectif de type fini de rang constant non nul et le morphisme $A \otimes_R A \to \prod_G A$ défini par $b \otimes a \mapsto (g(b)a)_{g\in G}$ est un isomorphisme de A-algèbres ;*
3. *[CHR] ou [DI] : $A^G = R$ et il existe des éléments $a_1, \ldots, a_n, b_1, \ldots, b_n$ dans A tels que*
$$\forall\ g, g' \in G \qquad \sum_{i=1}^{n} g(a_i)g'(b_i) = \delta_{g,g'}$$
4. *[CHR] ou [DI] : $A^G = R$ et le morphisme $A \otimes_R A \to \prod_G A$ défini par $b \otimes a \mapsto (g(b)a)_{g\in G}$ est un isomorphisme de A-algèbres ;*
5. *$A^G = R$ et (voir le théorème 10.1) pour tout idéal maximal $\mathfrak{p}' \subset A$, le morphisme canonique de groupes $D(\mathfrak{p}') \twoheadrightarrow \mathrm{Aut}_k\, k'$ est injectif (donc bijectif).*
6. *$A^G = R$ et (voir le corollaire 10.2) pour tout idéal maximal $\mathfrak{p}' \subset A$, l'application $G \twoheadrightarrow \mathrm{Hom}_R(A, A/\mathfrak{p}')$ est injective (donc bijective) ;*

Exemple 4.2 Soit E/K une extension galoisienne classique (de corps) de dimension finie et $G = \mathrm{Aut}_K E$. Bien sûr, l'extension E/K est une algèbre galoisienne de groupe G.

Considérons $R \subset K$ un anneau principal dont le corps des fractions est K, et notons A la fermeture intégrale de R dans E. Comme A est un R-module sans torsion, il est libre (donc projectif), et de rang $[E : K] = |G|$. Si le discriminant d'une base $(a_g)_{g\in G} \subset A$ de A/R est inversible dans R (cas dans lequel on peut toujours se retrouver quitte à localiser) alors A/R est une algèbre galoisienne de groupe G : en effet, comme le discriminant de la base $(a_t)_t$ est inversible, la matrice $M = \big(h(a_g)\big)_{g,h\in G}$ est inversible car $M.{}^tM$ est la matrice discriminant (inversible). De l'inversibilité de M, on déduit le fait que G est une base de $L_R(A,A)$ en utilisant le isomorphisme $L_R(A,A) \to A^{|G|}$ donné par $f \mapsto \big(f(a_g)\big)_{g\in G}$.

Exemple 4.3 Soit R un anneau (commutatif unitaire) dans lequel le discriminant du polynôme cyclotomique $\Phi_n(X)$ est inversible [1]. Alors $A = R[X]/\langle \Phi_n(X) \rangle$ est une R-algèbre galoisienne de groupe de Galois $G = \{\overline{X} \mapsto \overline{X}^k \mid k \in U(\mathbb{Z}/n\mathbb{Z})\}$: en effet, A est libre sur R (donc projectif) de type fini, si bien que $L_R(A, A)$ est isomorphe à A^d (où $d = \deg(\Phi_n)$) via $f \mapsto \big(f(1), f(\overline{X}), \ldots, f(\overline{X}^{d-1})\big)$. On montre que l'image du groupe G est une base de A^d car le déterminant de la matrice de Vandermonde $\left(g(\overline{X}^j)\right)_{\substack{g\in G \\ j=1\ldots d-1}}$ est une racine carrée de $\prod_{g\neq h\in G} \big(g(\overline{X}) - h(\overline{X})\big)$, c'est-à-dire du discriminant (inversible) de $\prod_{g\in G} \big(T - g(\overline{X})\big) = \prod_{k\in U(\mathbb{Z}/n\mathbb{Z})} \left(T - \overline{X}^k\right) = \Phi_n(T)$.

Exemple 4.4 Soit R un anneau (commutatif unitaire),

$$f = T^n - a_1 T^{n-1} + \cdots + (-1)^n a_n \quad \in R[T]$$

un polynôme unitaire de degré n, $X_1, \ldots, X_n$ des indéterminées sur R, pour $i = 1, \ldots, n$ on note σ_i le polynôme symétrique élémentaire homogène de degré i en les X_k, et enfin Σ l'idéal engendré par les relations symétriques des racines de f $\{\sigma_1 - a_1, \ldots, \sigma_n - a_n\}$ dans $R[X_1, \ldots, X_n]$.

On appelle le quotient $A = R[X_1, \ldots, X_n]/\Sigma$ l'*algèbre de décomposition universelle* de f sur R (voir [Bou4] p.68, ou [DQ]).

La R-algèbre A est galoisienne (de groupe $\mathcal{S}_n$, le groupe symétrique) si et seulement si le discriminant de f est inversible dans R (voir [Duc]).

Quelques implications entre les assertions de la définition 4.1

1. $\Rightarrow$ **3.** Voir la section 2

1. $\Rightarrow$ **2. ou 4.** Voir la section 3

3. $\Rightarrow$ **1.** On établit rapidement que A/R est projectif de type fini car, en posant $\mathrm{tr}(x) = \sum_{g\in G} g(x)$ pour tout $x \in A$, on a :

$$\sum_{i=1}^{n} \mathrm{tr}(a_i x) b_i = \sum_{i=1}^{n} \left(\sum_{g\in G} g(a_i x) \right) b_i = \sum_{g\in G} \delta_{g,\mathrm{Id}} g(x) = x$$

Ensuite on montre que G est A-libre dans $L_R(A, A)$. En effet, une combinaison linéaire nulle $\sum_{g\in G} a_g.g = 0$ implique $\sum_i \sum_{g\in G} a_g.g(a_i).h(b_i) = 0$ pour tout $h \in G$, d'où $0 = \sum_{g\in G} a_g \delta_{g,h} = a_h$ pour tout $h \in G$.

[1] La partie sans facteur carré de $\mathrm{dis}(\Phi_n(X))$ est égale à celle de n, sauf quand $n \equiv 2 \mod 4$. Dans ce cas exceptionel, $\Phi_n(X) = \Phi_{n/2}(-X)$ et son discriminant n'est pas multiple de 2. En clair, l'inversibilité de n est davantage restrictive que celle de $\mathrm{dis}(\Phi_n(X))$.

Enfin, l'ensemble G est générateur de $L_R(A,A)$ sur A : si $h \in L_R(A,A)$, poser $w_g = \langle g, h\rangle = \sum_i g(a_i)h(b_i)$, alors $h = \sum_g w_g g$. En effet, pour $x \in A$:

$$\sum_g w_g g(x) = \sum_i \sum_g h(b_i)g(a_i)g(x) = h\left(\sum_i \mathrm{tr}(a_i x)b_i\right) = h(x)$$

3. $\Rightarrow$ **6.** Soit $g \in G$ tel que $g \equiv \mathrm{Id} \mod \mathfrak{p}'$. On a alors

$$\delta_{g,\mathrm{Id}} = \sum_i g(a_i)b_i \equiv \sum_i a_i b_i = 1 \mod \mathfrak{p}'$$

donc $g = \mathrm{Id}$ et le morphisme $G \twoheadrightarrow \mathrm{Hom}_R(A, A/\mathfrak{p}')$ est injectif.

5. $\Rightarrow$ **6.** Soit $g \in G$ tel que pour tout $x \in A$ on ait $g(x) - x \in \mathfrak{p}'$. Alors pour tout $x \in \mathfrak{p}'$, on a $g(x) \in \mathfrak{p}'$, donc $g \in D(\mathfrak{p}')$. Comme $g \equiv \mathrm{Id} \mod \mathfrak{p}'$, le point 5. implique $g = \mathrm{Id}$.

6. $\Rightarrow$ **3.** Une traduction possible du point 6. est «$A^G = R$ et pour tout idéal maximal $\mathfrak{p}'$ et tout $g \in G$ distinct de Id, il existe au moins un $x \in A$ tel que $g(x) - x \notin \mathfrak{p}'$». Voir la démonstration dans [DI], page 84.

6. $\Rightarrow$ **5.** Comme $D(\mathfrak{p}') \subset G$, l'implication est évidente...

5 Idempotents et $\mathrm{Aut}_R(A)$

Proposition 5.1 *Soit A/R une algèbre galoisienne de groupe G et $(a_t)_t, (a_t^*)_t$ un système (fini) de coordonnées de A/R. Alors*

- *pour tout $f \in \mathrm{GL}_R(A)$, on a $\sum_t a_t^* \circ f^{-1} \otimes f(a_t) = \sum_t a_t^* \otimes a_t \quad \in A^* \otimes_R A$;*
- *si $f \in \mathrm{Hom}_R(A,A)$ et $s_g = \langle f, g\rangle$ pour tout $g \in G$ ($(s_g)_g$ est un s.f.i.o.), on a*

$$f \in \mathrm{Aut}_R(A) \iff \sum_{g\in G} g\left(s_{g^{-1}}\right) = 1 \iff \left\{g\left(s_{g^{-1}}\right)\right\}_{g\in G} \text{ s.f.i.o.}$$

  Si tel est le cas, alors $f^{-1} = \sum_{g\in G} g\left(s_{g^{-1}}\right) g$;
- *pour tout $f \in \mathrm{Aut}_R(A)$, on a $\mathrm{tr} \circ f = \mathrm{tr}$;*
- *si $f \in \mathrm{Aut}_R(A)$ alors $u \mapsto u \circ f^{-1}$ est un A-automorphisme de $L_R(A,A)$ (muni de $*$),* i.e. *pour tout $v, w \in L_R(A,A)$ on a $(v \circ f^{-1}) * (w \circ f^{-1}) = (v * w) \circ f^{-1}$.*
  En particulier $\langle v \circ f^{-1}, w \circ f^{-1}\rangle = \langle v, w\rangle$, i.e. *$u \mapsto u \circ f^{-1}$ est un opérateur orthogonal de $L_R(A,A)$.*

Démonstration Soit $f \in \mathrm{Hom}_R(A,A)$ et $(s_g)_{g\in G}$ le s.f.i.o. tel que $f = \sum_{g\in G} s_g g$. Considérons l'application R-linéaire $u = \sum_{h\in G} h(s_{h^{-1}})h$ et composons :

$$\begin{aligned} u \circ f &= \sum_{h,g\in G} h(s_{h^{-1}})h(s_g)hg = \sum_{h,g\in G} h(s_{h^{-1}}s_g)hg \\ &= \sum_{h,g\in G} h(\delta_{h^{-1},g}s_{h^{-1}})hg = \sum_{h\in G} h\left(s_{h^{-1}}\right)\mathrm{Id} \end{aligned}$$

En clair, si $\sum_h h\left(s_{h^{-1}}\right) = 1$ alors f est inversible, d'inverse u donc $\{h\left(s_{h^{-1}}\right)\}_{h\in G}$ est un système fondamental d'idempotents orthogonaux.

Considérons un système (fini) de coordonnées $(a_t)_t$, $(a_t^*)_t$ de A sur R, *i.e.* pour tout $x \in A$, $x = \sum_t a_t^*(x)a_t$, et une application $f \in \mathrm{GL}_R(A)$. On constate facilement que $\left(c_t = f(a_t)\right)_t$, $\left(c_t^* = a_t^* \circ f^{-1}\right)_t$ est également un système de coordonnées : soit $y \in A$ et $x = f^{-1}(y)$

$$\sum_t c_t^*(y)c_t = \sum_t a_t^*(x)f(a_t) = f\left(\sum_t a_t^*(x)a_t\right) = f(x) = y$$

ce qui montre que $\sum_t a_t^* \circ f^{-1} \otimes f(a_t) = \sum_t a_t^* \otimes a_t$. Si $f \in \mathrm{Aut}_R(A)$ alors

$$\mathrm{tr}(f^{-1}(x)) = \sum_t a_t^*(f^{-1}(x)a_t) = \sum_t c_t^*(xc_t) = \mathrm{tr}(x)$$

Remarque. En écrivant $\mathrm{tr} = \mathrm{tr} \circ f$ avec $f = \sum_g s_g g$, on obtient

$$\sum_{h\in G} h = \sum_{k,g\in G} k(s_g)kg = \sum_{h,g\in G} h(g^{-1}(s_g))h$$

d'où, par identification sur la base $G \in L_R(A,A)$, $1 = h^{-1}(1) = \sum_g g^{-1}(s_g)$.

Maintenant que (classiquement) deux éléments f-conjugués ont même trace, on peut transporter l'action de f sur A en une action de f sur $A \otimes_R A$, puis sur $L_R(A,A)$, ce qui donne $f.u = u \circ f^{-1}$ pour tout $u \in L_R(A,A)$ (voir remarque page 8). Comme f est un R-automorphisme de A, $u \mapsto u \circ f^{-1}$ est un A-automorphisme de $L_R(A,A)$ (muni de $*$). Ceci a pour conséquence

$$\begin{array}{rcl} (v \circ f^{-1}) * (w \circ f^{-1}) & = & (v * w) \circ f^{-1} \\ \langle v \circ f^{-1}, w \circ f^{-1}\rangle & = & (v \circ f^{-1}) * (w \circ f^{-1})(1) \\ & = & (v * w) \circ f^{-1}(1) = (v * w)(1) = \langle v, w\rangle \end{array}$$ □

Propriété 5.2 *Soit A/R une algèbre galoisienne de groupe G.*

- *Si les idempotents de A appartiennent à R, alors* $\mathrm{Aut}_R(A) = \mathrm{Hom}_R(A,A)$. *Voir [CHR] (p.25-26)*
  En particulier, si $0, 1$ sont les seuls idempotents de A alors $G = \mathrm{Hom}_R(A,A)$. Voir [DI] (p.88-89)
- *si 0 et 1 sont les seuls idempotents de R et G abélien alors tout homomorphisme $f \in \mathrm{Hom}_R(A,A)$ commutant avec les éléments de G appartient à G. Voir [Len] (p.4)*

Démonstration

- Utiliser la propriété 3.2 et la proposition 5.1 : on obtient sans difficulté qu'un élément $\sum_g s_g g$ de $\mathrm{Hom}_R(A,A)$ est inversible lorsque tous les s_g appartiennent à R puisque $g\left(s_{g^{-1}}\right) = s_{g^{-1}}$.
  Si 0 et 1 sont les seuls idempotents de A, alors un élément $f \in \mathrm{Hom}_R(A,A)$ s'écrit $\sum_g \langle f, g\rangle g$ avec $\langle f, g\rangle = 0$ pour tout g sauf $\langle f, g_0\rangle = 1$, donc $f = g_0$.

– Soit $f \in \mathrm{Hom}_R(A, A)$ commutant avec tout élément de G (supposé abélien). Alors, pour $h \in G$, il vient

$$\sum_{g\in G} \langle f, g\rangle\, hg = \sum_{g\in G} \langle f, g\rangle\, gh = fh = hf = \sum_{g\in G} h(\langle f, g\rangle)hg$$

Comme G est A-libre, on a $\langle f, g\rangle = h(\langle f, g\rangle)$ pour tout $h \in G$, donc les idempotents $(\langle f, g\rangle)_g$ appartiennent à R. Par conséquent, ils sont tous nuls sauf un seul, si bien que f appartient à G. □

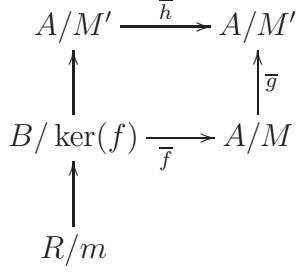
6 Étude de $\mathrm{Hom}_R(B, A/M)$

Proposition 6.1 *Soit A/R une algèbre galoisienne de groupe G et H un sous-groupe de G. Pour une sous-algèbre $B \subset A$ et un idéal maximal $M \subset A$, on note $\mathrm{Hom}_R(B, A/M)$ l'ensemble des homomorphismes de R-algèbres de B dans le corps A/M. Alors*

- *les éléments de $\mathrm{Hom}_R(B, A/M)$ sont de la forme $(g|_B \mod M)$ avec $g \in G$;*
- *l'application $(G/H)_g \to \mathrm{Hom}_R(A^H, A/M)$ qui envoie $g.H$ sur $(g|_{A^H} \mod M)$ est injective (donc bijective).*

Démonstration Soit M un idéal maximal de A. D'après le corollaire 10.2, on sait que le morphisme $G \to \mathrm{Hom}_R(A, A/M)$ (qui envoie $g \in G$ sur $g \mod M$) est surjectif. Pour B une sous-R-algèbre et $f \in \mathrm{Hom}_R(B, A/M)$, on considère un idéal maximal M' de A contenant l'idéal maximal $\ker(f)$ de B.

Cet idéal M' contient entre autres les éléments $r \in m = R \cap M$ car $f(r) = r.f(1) = r.1 \mod M = 0 \mod M$, donc M' et M sont G-conjugués (voir le théorème 10.1). Disons $M' = g(M)$, et ainsi g induit un isomorphisme $\overline{g} : A/M \to A/M'$. On alors prolonger $\overline{g} \circ \overline{f} : B/\ker(f) \to A/M'$ en un élément de $\mathrm{Aut}_{R/m}(A/M')$, ce dernier étant de la forme $\overline{h} = h \mod M'$ avec $h \in D(M')$ (voir le théorème 10.1).
Finalement $f = (g^{-1} \circ h) \mod M$



Dans le cas particulier où $B = A^H$ (un sous-anneau de points fixes), on connaît exactement le « noyau » de l'application surjective $G \twoheadrightarrow \mathrm{Hom}_R(A^H, A/M)$ qui envoie g sur $g|_{A^H} \mod M$. En effet, si $g \equiv \mathrm{Id} \mod M$, alors $g \mod M$ est un élément de $\mathrm{Hom}_{A^H}(A, A/M)$. Comme A est galoisienne sur A^H, il existe $h \in H$ tel que $h \mod M \equiv g \mod M$. Mais d'après l'une des assertions de la définition 4.1, le morphisme canonique $G \to \mathrm{Hom}_R(A, A/M)$ est injectif, donc $g = h \in H$.

Ceci prouve que $\mathrm{Hom}_R(A^H, A/M)$ est en bijection avec $(G/H)_g$, ce qui munit en particulier $\mathrm{Hom}_R(A^H, A/M)$ d'une structure de G-ensemble homogène. □

Proposition 6.2 *Avec les mêmes notations et hypothèses que la proposition 6.1, en posant de plus $H = \mathrm{Fix}_G(B)$, les assertions suivantes sont équivalentes :*

1. $B = A^H$;
2. *pour tout idéal maximal* $M \subset A$ *et pour tout* $g \in G$,

$$[\forall\ x \in B,\ g(x) = x \mod M] \Rightarrow [\forall\ x \in B,\ g(x) = x]\,;$$

(assertion triviale à l'évidence si A *est un corps) ;*

3. *pour tout idéal maximal* $M \subset A$, *l'application*

$$\begin{array}{ccc} (G/H)_g & \longrightarrow & \mathrm{Hom}_R(B, A/M) \\ g.H & \longmapsto & g|_B \mod M \end{array}$$

est injective (donc bijective) ;

4. *le cardinal de* $\mathrm{Hom}_R(B, A/M)$ *est* $[G : H]$.

On obtient alors une correspondance galoisienne entre les sous-groupes de G *et les sous-algèbres* $B \subset A$ *vérifiant l'une des assertions ci-dessus (par exemple l'assertion 2, triviale dans le cadre des corps) :*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \textit{sous-algèbres} \\ \mid \textit{assertion 2} \end{array} \right\} & \longleftrightarrow & \{\textit{sous-groupes de } G\} \\ B & \longmapsto & \mathrm{Fix}_G(B) \\ A^H & \longleftarrow & H \end{array}$$

À comparer avec la correspondance "classique" donnée dans [CHR] (p.24) ou [FP] (p.402) entre les sous-groupes de G *et les sous-algèbres « séparables et* G*-strong », ou encore, dans une autre mesure, celle de [VZ] entre les sous-algèbres « projectives séparables » et les « fat subgroups » de* $\mathrm{Aut}_R(A)$ *tout entier, sous condition que* R *ait un nombre fini d'idempotents...*

Démonstration Une partie du résultat est déjà démontrée ci-dessus et il reste à démontrer que la dernière assertion implique la première. Considérons une sous-R-algèbre $B \subset A^H$ en supposant que le cardinal $\mathrm{Hom}_R(B, A/M)$ soit $[G : H]$. Notons $m = M \cap R$, puis

$$\overline{R} = R/m\ \subset\ \overline{B} = B/(m.A \cap B)\ \subset\ \overline{A^H} = A^H/(m.A \cap A^H)\ \subset\ \overline{A} = A/m.A$$

Nous avons démontré plus haut que m est inclus dans le noyau de tout homomorphisme de $\mathrm{Hom}_R(B, A/M)$ (de la forme $g \mod M$), donc

$$\mathrm{Hom}_R(B, A/M) \subset \mathrm{Hom}_{\overline{R}}(\overline{B}, A/M)$$

Ainsi, en sachant que $\overline{A}$ est une algèbre galoisienne sur le corps $\overline{R}$ de groupe G, et $\overline{A}^H = \overline{A^H}$, on obtient :

$$[G : H] = \#\,\mathrm{Hom}_R(B, A/M) \leqslant \#\,\mathrm{Hom}_{\overline{R}}(\overline{B}, A/M) \leqslant [\overline{B} : \overline{R}] \leqslant [\overline{A^H} : \overline{R}] = [G : H]$$

d'où $\overline{B} = \overline{A^H}$, ou encore $A^H = B + (m.A \cap A^H)$. D'autre part, $m.A \cap A^H = m.A^H$ (voir [Len]), donc $A^H = B + m.A^H$ et ce quel que soit $m = M \cap R$ idéal maximal de R. La proposition 11.4 permet de conclure $B = A^H$. □

7 Action de G sur $\mathrm{Hom}_R(A^H, A/M)$

? ? ?

8 Éléments invariants

Définition 8.1 *Un polynôme à coefficients dans un anneau commutatif est dit* ***séparable*** *si son discriminant est inversible.*

Définition 8.2 *Soit A un anneau commutatif sur lequel opère un groupe fini G et le sous-anneau des points fixes $R = A^G$. Pour tout élément $x \in A$, on définit la* ***résolvante*** *$\mathbb{L} \in R[T]$ associées à x par*

$$\mathbb{L}(T) = \prod_{y \in G.x} (T - y)$$

Proposition 8.3 *Soit A une algèbre galoisienne sur R de groupe G. On considère un élément $x \in A$ dont la résolvante $\mathbb{L}$ est supposée séparable, $E \subset G.x$ de cardinal d, et s_i l'évaluation en E du i^epolynôme symétrique élémentaire homogène de degré $1 \leqslant i \leqslant d$, alors :*

- *$A^H = R[s_1, \ldots, s_d]$ où $H = \mathrm{Stab}_G(E)$;*
- *en particulier, $A^{\mathrm{Fix}_G(x)} = R[x]$ est libre sur R, de base $\{1, x, \ldots, x^{d-1}\}$, et $\mathbb{L}$ est le polynôme minimal de x sur R ;*
- *en particulier, si $A = R[x]$ et $E = H.x$ où $H \subset G$, alors $A^H = R[s_1, \ldots, s_d]$.*

Démonstration Avec les notations de cette proposition, posons $B = R[s_1, \ldots, s_d]$. Comme $H = \mathrm{Stab}_G(E)$ et que s_i est l'évaluation en E du i^epolynôme symétrique, on peut conclure que s_i est fixé par tout élément de H, i.e. $B \subset A^H$.

Soit M un idéal maximal de A. Comme $\mathbb{L} = \prod_{y \in G.x}(T - y)$ est séparable, i.e. $\prod_{\substack{y,z \in G.x \\ y \neq z}} (y - z)$ inversible, il est clair que $\prod_{\substack{y,z \in G.x \\ y \neq z}} (y - z) \neq 0 \mod M$ et donc que $G.x \mod M$ est de même cardinal que $G.x$. En particulier, $G.x \ni y \mapsto y \mod M$ est injective...

Maintenant considérons $g \in G$ tel que $g|_B = \mathrm{Id}\,|_B \mod M$. Alors $g(s_i) = s_i \mod M$ donc $g(E) = E \mod M$ car $E \mod M$ est l'ensemble des racines du polynôme $T^d - s_1 T^{d-1} + \cdots + (-1)^d s_d \mod M$. Or $G.x \ni y \mapsto y \mod M$ est injective, donc $g(E) = E$, et finalement $g \in H$.

Ainsi, quel que soit l'idéal maximal M, on a $\mathrm{Hom}_R(B, A/M) = (G/H)_g$ (voir la proposition 6.2) et $B = A^H$.

Si de plus on considère la cas particulier où $E = \{x\}$, alors $H = \mathrm{Fix}_G(x)$ et on obtient $R[x] = A^{\mathrm{Fix}_G(x)}$.

Remarque. On démontre également la réciproque : si $R[x] = A^{\mathrm{Fix}_G(x)}$ alors la résolvante de x est séparable. En effet, si $R[x] = A^H$ alors x est un générateur de A^H modulo tout idéal maximal de A, donc sa résolvante $\mathbb{L}$ est séparable modulo tout idéal maximal. Le discriminant de $\mathbb{L}$ ne peut donc pas être autre qu'un inversible de A.

Montrons que $\mathbb{L}$ est le polynôme minimal de x sur R. Soit $P(T) \in R[T]$ s'annulant en x. Alors pour tout $g \in G$, on a $0 = g(P(x)) = P(g(x))$. Donc $T - y$ divise $P(T)$ quel que soit $y \in G.x$. Or dis($\mathbb{L}$) est inversible donc $y - z$ est régulier dans A pour $y, z \in G.x$ ($y \neq z$). Ainsi $\prod_{y \in G.x}(T - y)$ divise P, i.e. $\mathbb{L}$ est le polynôme minimal de x sur R. Par suite, $R[x] \simeq R[T]/\langle \mathbb{L} \rangle$ est libre dont la base canonique est $\{1, x, \ldots, x^{d-1}\}$.

Remarque. Pour établir ce résultat, on utilise uniquement, outre la définition de $\mathbb{L}$, que $A^G = R$ et dis($\mathbb{L}$) régulier dans A.

Encore plus particulier est le cas où $R[x] = A$... Soit E l'orbite de x sous l'action d'un sous-groupe H de G. Alors $H \subset \mathrm{Stab}_G(E)$ puisque H stabilise E. Réciproquement, si $g \in G$ stabilise E, alors $g(x)$ appartient à E, donc $g(x) = h(x)$ avec $h \in H$. Comme x est un générateur de A/R, on a $g = h \in H$. Ainsi $H = \mathrm{Stab}_G(E)$, et donc $A^H = R[s_1, \ldots, s_d]$. □

9 Groupes cohomologiques $H^q(G, A)$ et $H^1(G, A^\times)$

Proposition 9.1 (voir [CHR] p.31 ou [DI] p.116) *Soit A/R une algèbre galoisienne de groupe de Galois G. On note $A^\times$ le groupe multiplicatif des inversibles de A. Alors*

- *le groupe cohomologique $H^1(G, A)$ est trivial ;*
- *les groupes cohomologiques $H^q(G, A)$ sont triviaux pour $q \geqslant 2$;*
- *le groupe cohomologique $H^1(G, A^\times)$ est trivial si R est un corps ;*
- *pour tout 1-cocyle $(c_g)_{g \in G}$ de $H^1(G, A^\times)$, il existe un élément régulier $a \in A$ tel que pour tout $g \in G$ on ait $c_g = g(a)/a$.* ? ? ?

Démonstration On a $\mathrm{tr}(A) = R$ (car $A = \mathrm{tr}(A).A$). Par suite le groupe cohomologique $H^1(G, A)$ est trivial : en effet, pour tout 1-cocyle $(a_g)_{g \in G}$, i.e. vérifiant la relation $a_{gh} = a_g + g(a_h)$, on a $a_h = a - h(a)$ (cobord) avec $a = \displaystyle\sum_{g \in G} a_g g(c)$ où c est un élément quelconque de trace 1.

D'autre part, on peut démontrer qu'en fait tous les groupes $H^q(G, A)$ sont triviaux : en effet, A s'injecte dans $L_R(A, A)$ via $\phi \ : \ a \mapsto \mathrm{tr}(a\cdot) = \sum_g g(a).g$ (voir la section 2). On remarque que l'image $\widetilde{A}$ de A est un facteur direct de $L_R(A, A)$ car l'injection ϕ possède une section $L_R(A, A) \to A$ définie par $f \mapsto \langle \mathrm{Id}, f \rangle$.

De plus, les actions de G sur $A \simeq \widetilde{A}$ et sur $L_R(A, A)$ sont compatibles avec ϕ et sa section (voir page 8) :

$$\begin{array}{cc} \forall\ a \in A & g.a = g(a) \\ \forall\ f \in L_R(A, A) & g.f = f \circ g^{-1} \end{array}$$

Ainsi on démontre que $A \simeq \widetilde{A}$ est un facteur direct de $L_R(A,A)$ en tant que G-modules.

Enfin $G \subset L_R(A,A)$ est une A-base normale, donc $L_R(A,A)$ est un *G-module induit*, et par suite A est un *G-module relativement projectif*. Comme le groupe G est fini, il y a coïncidence entre les notions de *G-modules induits* et *co-induits*, et de même pour les *G-modules relativement projectifs* et *relativement injectifs* (voir [Ser], p.118). Or la cohomologie des *G-modules relativement injectif* est triviale (voir [Ser], p.120), ce qui montre que $H^q(G,A) = \{0\}$.

A TERMINER □

10 Rappels sur A/A^G

Théorème 10.1 (voir [Bou3], p.40) *Soit A un anneau commutatif, G un groupe fini opérant sur A, R l'anneau des invariants sous l'action de G. Alors*

- *A est entier sur R.*
- *G opère transitivement sur les idéaux premiers de A au-dessus d'un même idéal premier de R. Autrement dit, si $\mathfrak{p}'$ et $\mathfrak{q}'$ sont deux idéaux premiers de A tel que $\mathfrak{p}' \cap R = \mathfrak{q}' \cap R$, alors $G.\mathfrak{p}' = G.\mathfrak{q}'$.*
- *Soit $\mathfrak{p}'$ un idéal premier de A, $\mathfrak{p} = R \cap \mathfrak{p}'$ idéal premier de R, k le corps des fractions de $R/\mathfrak{p}$ et k' celui de $A/\mathfrak{p}'$. Alors k' est une extension normale de k et le morphisme canonique de $D(\mathfrak{p}') = \mathrm{Stab}_G \mathfrak{p}' = \{g \in G \mid g\mathfrak{p}' = \mathfrak{p}'\}$ dans le groupe $\mathrm{Aut}_k k'$ est surjectif* [...]

Corollaire 10.2 (voir [Bou3], p.42) *Les hypothèses et les notations étant celles du théorème 10.1, soit f_1, f_2 deux homomorphismes de A dans un corps L ayant même restriction à R. Alors il existe $g \in G$ tel que $f_2 = f_1 \circ g$.*

Une conséquence de ce corollaire est que pour tout idéal maximal $\mathfrak{p}'$ de A, l'application canonique $G \to \mathrm{Hom}_R(A, A/\mathfrak{p}')$ définie par $g \mapsto \overline{g} = \pmod{\mathfrak{p}'} \circ g$ est surjective.

11 Rappels sur le(s) lemme(s) de Nakayama

Dans ce qui suit, A désigne un anneau commutatif et E un A-module de type fini.

Lemme 11.1 (voir [Lan], p.424) *Soit a un idéal de A contenu dans le radical de Jacobson de A, i.e. l'intersection de tous les idéaux maximaux de A. Si $a.E = E$ alors $E = (0)$.*

Lemme 11.2 (voir [Lan], p.425) *Si A est local d'idéal maximal m, et F un sous-A-module de E tel que $E = F + m.E$, alors $F = E$.*

Lemme 11.3 (voir [Lan], p.425) *Si A est local d'idéal maximal m, alors tout système, générateur de $E \mod m.E$, est un système générateur de E.*

Proposition 11.4 *Soit F un sous-A-module de E tel que $E = F + m.E$ pour tout idéal maximal m de A. Alors $F = E$.*

Démonstration Pour tout idéal maximal m de R, on a $m.E/F = (F + m.E)/F = E/F$. Si on localise en $A \setminus m$ (donnant naissance à A_m, E_m et F_m), on obtient $(mA_m).(E_m/F_m) = E_m/F_m$. Ainsi, $E_m/F_m = (0)$ pour tout idéal maximal $m \subset A$. Ceci implique que $E/F = (0)$ (i.e. $E = F$) : en effet, pour tout $x \in E/F$, quel que soit m maximal, il existe $s \notin m$ tel que $s.x = 0$. Ainsi $\mathrm{Ann}_A(x) = A$... □

Références

[Bou1] N. Bourbaki. *Algèbre commutative,* ch. 1, Modules plats. Hermann, 1961.

[Bou2] N. Bourbaki. *Algèbre,* ch. 2, Algèbre linéaire. Hermann, 1962.

[Bou3] N. Bourbaki. *Algèbre commutative,* ch. 5, Entiers. Hermann, 1964.

[Bou4] N. Bourbaki. *Algèbre,* ch. 4, Polynômes et fractions rationnelles. Masson, 1981.

[CHR] S.U. Chase, D.K. Harrison, and A. Rosenberg. Galois Theory and Galois Cohomology of Commutative Rings. *Memoirs of the American Mathematical Society*, 52 :15–33, 1965.

[DI] F. DeMeyer and E. Ingraham. Separable algebras over commutative rings, ch. 3. *Lecture notes in Mathematics, 181, Springer-Verlag, Berlin*, 1971.

[DQ] L. Ducos and C. Quitté. Algèbre de décomposition universelle, Implémentation et applications à la théorie de Galois. Prépublication de l'Université de Poitiers, n.98, juin 1996.

[Duc] L. Ducos. *Effectivité en théorie de Galois. Sous-résultants.* Université de Poitiers, 1997. Thèse doctorale.
`www-math.univ-poitiers.fr/~ducos`.

[FP] M. Ferrero and A. Paques. Galois Theory of Commutative Rings Revisited. *Contributions to Algebra and Geometry*, 238(2) :399–410, 1997.

[Lan] S. Lang. *Algebra, third edition.* Addison-Wesley publishing compagny, Inc., 1993.

[Len] H.W. Lenstra. Galois Theory and Primality Testing. *Lecture notes in Mathematics, 1142, Springer-Verlag, Berlin, New-York*, pages 169–189, 1985.

[Ser] J.P. Serre. *Corps locaux.* Hermann, 1962.

[VZ] O. E. Villamayor and D. Zelinsky. Galois Theory for Rings with Finitely many Idempotents. *Nogoya Math. Journal*, 27 :721–731, 1966.