L'algèbre de décomposition universelle

Gema M. Diaz–Toca ([1]), Henri Lombardi ([2]), Claude Quitté ([3])

2006

Résumé

On donne les principales propriétés de l'algèbre de décomposition universelle d'un polynome et on l'applique pour un traitement constructif du corps des racines d'un polynome.

Introduction

Toutes les algèbres qu'on considère sont associatives, commutatives et avec élément neutre. Il revient donc au même de se donner une $\mathbf{A}$-algèbre $\mathbf{C}$ ou un homomorphisme $\mathbf{A} \xrightarrow{\rho} \mathbf{C}$.

Nous étudions l'algèbre de décomposition universelle d'un polynome unitaire sur un anneau commutatif arbitraire.

> Dans tout cet article, $\mathbf{A}$ est un anneau commutatif, $f = T^n + \sum_{k=1}^{n}(-1)^k a_k T^{n-k} \in \mathbf{A}[T]$ et $\mathbf{B} = \mathrm{Adu}_{\mathbf{A},f}$ est l'algèbre de décomposition universelle de f sur $\mathbf{A}$.

Dans la section 1 nous introduisons les modules de Cauchy et la base classique correspondante de l'algèbre de décomposition universelle. Nous montrons que les deux définitions naturelles de la norme coïncident.

Dans la section 2 nous introduisons les notions d'idempotent galoisien (un idempotent dont l'orbite sous S_n est un système fondamental d'idempotents orthogonaux), d'algèbre prégaloisienne, de quotient de Galois d'une algèbre prégaloisienne. Une algèbre prégaloisienne est une algèbre qui vérifie un bon nombre de propriétés des algèbres galoisiennes, sans la condition de séparabilité. Le prototype d'une algèbre prégaloisienne est une algèbre de décomposition universelle, ou un quotient de Galois d'une algèbre de décomposition universelle.

Dans la section 3 nous montrons comment calculer des éléments galoisiens dans une algèbre de Boole munie d'un groupe d'automorphismes. Ceci s'applique en particulier à l'algèbre de Boole des idempotents d'une algèbre de décomposition universelle ou plus généralement d'une algèbre prégaloisienne.

Dans la section 4 nous montrons constructivement quelques propriétés importantes qui apparaissent sous l'hypothèse de séparabilité du polynome servant à construire l'algèbre de décomposition universelle. Nous montrons que l'algèbre de décomposition universelle est alors réduite si l'anneau de base est réduit, et plus généralement que le nilradical de $\mathbf{B}$ est engendré par celui de $\mathbf{A}$. Nous donnons sous une forme très précise le résultat qui affirme que « l'algèbre de décomposition universelle de diagonalise elle-même lorsque le polynome est séparable ». Nous améliorons aussi les résultats connus concernant les points fixes d'une algèbre de décomposition universelle (sous l'action de S_n) dans le cas où le polynome n'est pas supposé séparable.

Dans la section 5 nous généralisons un résultat de Aubry et Vallibouze concernant la structure « triangulaire » des idéaux galoisiens.

[1] Dpto. de Matematicas Aplicada Universidad de Murcia, Spain `gemadiaz@um.es`

[2] Laboratoire de Mathématiques de Besançon, CNRS UMR 6623, Université de Franche-Comté, 25 030 BESANCON cedex, FRANCE, `henri.lombardi@univ-fcomte.fr`

[3] Laboratoire de Mathématiques, SP2MI, Boulevard 3, Teleport 2, BP 179, 86960 FUTUROSCOPE Cedex, FRANCE, `quitte@mathlabo.univ-poitiers.fr`

Dans la section 6, pour étudier constructivement le « corps des racines » d'un polynome $f \in \mathbf{K}[T]$ (où $\mathbf{K}$ est un corps discret), alors que l'existence d'un tel corps n'est pas assurée d'un point de vue constructif, nous proposons d'utiliser des « approximations » de ce corps qui sont des quotients convenables de l'algèbre de décomposition universelle associée à f. Dans l'article [6] le premier auteur a donné dans le même esprit un traitement de la théorie de Galois d'un polynome séparable sur un corps discret en calcul formel. Cette étude du corps des racines « par approximations successives » peut être considérée comme une variante du système D5 [4] de traitement de la cloture algébrique en Calcul formel, ou encore comme la version constructive de l'approche de Bourbaki dans [3].

Puisque l'article est écrit dans le style des mathématiques constructives à la Bishop ([2, 10]) tous les théorèmes ont un contenu algorithmique. La terminologie constructive spécifique non précisée se trouve dans [10].

Remerciements. Nous remercions Thierry Coquand pour ses conseils judicieux.

1 Modules de Cauchy et base canonique

On notera $\mathbf{B} = \mathrm{Adu}_{\mathbf{A},f}$ l'*algèbre de décomposition universelle de f sur $\mathbf{A}$* définie comme suit :

$$\mathbf{B} = \mathrm{Adu}_{\mathbf{A},f} = \mathbf{A}[X_1,\dots,X_n]/\mathcal{J}(f) = \mathbf{A}[x_1,\dots,x_n]$$

où $\mathcal{J}(f)$ est l'idéal nécessaire pour identifier $\prod_{i=1}^n (T-x_i)$ avec $f(T)$ dans le quotient. Précisément considérons les fonctions symétriques élémentaires des X_i :

$$\alpha_1 = \sum\nolimits_{i=1}^{n} X_i,\ \alpha_2 = \sum\nolimits_{1\le i<j\le n} X_iX_j,\ \dots,\ \alpha_n = \prod\nolimits_{i=1}^{n} X_i\,.$$

Alors l'idéal $\mathcal{J}(f)$ est donné par :

$$\mathcal{J}(f) = \langle a_1-\alpha_1,\ a_2-\alpha_2,\dots,\ a_n-\alpha_n\rangle\,.$$

L'algèbre de décomposition universelle peut être caractérisée par la propriété suivante, qui est évidente.

Fait 1.1 (propriété caractéristique)
Soit $\mathbf{C}$ une $\mathbf{A}$-algèbre pour laquelle $f(T)$ se décompose en produit de facteurs $(T-z_i)$. Alors il existe un unique homomorphisme de $\mathbf{K}$-algèbres $\mathbf{B}\to\mathbf{C}$ qui envoie les x_i sur les z_i. Ceci caractérise l'algèbre de décomposition universelle $\mathbf{B} = \mathrm{Adu}_{\mathbf{A},f}$, à isomorphisme unique près.

Si en outre $\mathbf{C}$ est engendrée (comme $\mathbf{A}$-algèbre) par les z_i elle est isomorphe à un quotient de $\mathbf{B}$, la classe de x_i correspondant à z_i. Et en prenant $\mathbf{C} = \mathbf{B}$ on obtient que toute permutation des x_i produit un (unique) automorphisme de $\mathbf{B}$.

Dit autrement : le groupe S_n des permutations de $\{X_1,\dots,X_n\}$ agit sur $\mathbf{A}[X_1,\dots,X_n]$ et fixe l'idéal $\mathcal{J}(f)$, donc l'action passe au quotient et ceci définit S_n comme groupe d'automorphismes de l'algèbre de décomposition universelle.

Par changement d'anneau de base, on obtient comme conséquence du fait 1.1 le fait suivant.

Fait 1.2 (changement d'anneau de base)
Soit $\rho : \mathbf{A}\to\mathbf{A}_1$ une $\mathbf{A}$-algèbre. Notons $\rho(f)$ l'image de f dans $\mathbf{A}_1[T]$. Alors l'algèbre $\mathrm{Adu}_{\mathbf{A},f}\otimes_{\mathbf{A}}\mathbf{A}_1$, est naturellement isomorphe à $\mathrm{Adu}_{\mathbf{A}_1,\rho(f)}$.

Pour étudier l'algèbre de décomposition universelle on introduit les « modules de Cauchy » qui sont les polynomes suivants :

$$\begin{aligned}
f_1(X_1) &= f(X_1)\\
f_2(X_1,X_2) &= (f_1(X_1)-f_1(X_2))/(X_1-X_2)\\
&\vdots\\
f_{k+1}(X_1,\dots,X_{k+1}) &= (f_k(X_1,\dots,X_{k-1},X_k)-f_k(X_1,\dots,X_{k-1},X_{k+1}))/(X_k-X_{k+1})\\
&\vdots\\
f_n(X_1,\dots,X_n) &= (f_{n-1}(X_1,\dots,X_{n-2},X_{n-1})-f_{n-1}(X_1,\dots,X_{n-2},X_n))/(X_{n-1}-X_n)
\end{aligned}$$

Par exemple avec $n = 4$:

$$\begin{aligned}
f_1(x) &= x^4 - a_1x^3 + a_2x^2 - a_3x + a_4\\
f_2(x,y) &= (y^3 + y^2x + yx^2 + x^3) - a_1(y^2 + yx + x^2) + a_2(y + x) - a_3\\
&= y^3 + y^2(x - a_1) + y(x^2 - a_1x + a_2) + (x^3 - a_1x^2 + a_2x - a_3)\\
f_3(x,y,z) &= (z^2 + y^2 + x^2 + zy + zx + yx) - a_1(z + y + x) + a_2\\
&= z^2 + z(y + x - a_1) + ((y^2 + yx + x^2) - a_1(y + x) + a_2)\\
f_4(x,y,z,t) &= t + z + y + x - a_1
\end{aligned}$$

Ou pour $f(x) = x^6$:

$$\begin{aligned}
f_2(x,y) &= y^5 + y^4x + y^3x^2 + y^2x^3 + yx^4 + x^5\\
f_3(x,y,z) &= (z^4 + y^4 + x^4) + (z^2y^2 + z^2x^2 + y^2x^2)+\\
&\quad (zy^3 + zx^3 + yz^3 + yx^3 + xz^3 + xy^3) + (zyx^2 + zxy^2 + yxz^2)\\
f_4(x,y,z,t) &= (t^3 + z^3 + y^3 + x^3) + (tzy + tyx + tzx + zyx)+\\
&\quad (t^2(z + y + x) + z^2(t + y + x) + y^2(t + z + x) + x^2(t + z + y))\\
f_5(x,y,z,t,u) &= (u^2 + t^2 + z^2 + y^2 + x^2) + (xu + xt + xz + xy + tu + zu + zt + yu + yt + yz)\\
f_6(x,y,z,t,u,v) &= v + u + t + z + y + x
\end{aligned}$$

Plus généralement, pour $f(t) = t^n$, $f_k(t_1, \ldots, t_k)$ est la somme de tous les monomes de degré $n+1-k$ en $t_1, \ldots, t_k$. Ceci permet par linéarité d'obtenir un description précise explicite des modules de Cauchy pour un polynome arbitraire.

Le polynome f_i est symétrique en les variables $X_1, \ldots, X_i$, unitaire en X_i, de degré total $n - i + 1$.

Le fait 1.1 implique que l'idéal $\mathcal{J}(f)$ est égal à l'idéal engendré par les modules de Cauchy. Donc l'algèbre de décomposition universelle est un $\mathbf{A}$-module libre de rang $n!$:

Fait 1.3 *Le $\mathbf{A}$-module $\mathbf{B}$ est libre et une base est formée par les « monomes » $x_1^{d_1} \cdots x_{n-1}^{d_{n-1}}$ tels que pour $k = 1, \ldots, n-1$ on ait $d_k \leq n - k$. Nous noterons cette base $\mathcal{B}(f)$.*

Dans le cas où $\mathbf{A}$ est un corps discret, les modules de Cauchy peuvent être vus comme une base de Gröbner de l'idéal, pour l'ordre monomial lexicographique avec $X_1 < X_2 < \cdots < X_n$.

En fait même si $\mathbf{A}$ n'est pas un corps discret, les modules de Cauchy fonctionnent comme une base de Gröbner : tout polynome en les x_i se réécrit sur la base de monomes précédente par divisions successives par les modules de Cauchy. On divise tout d'abord par f_n par rapport à la variable X_n, ce qui la fait disparaître. Ensuite on divise par f_{n-1} par rapport à la variable X_{n-1}, ce qui la ramène en degré ≤ 1, et ainsi de suite.

On peut donner une explication plus précise pour le fait que l'idéal $\mathcal{J}(f)$ est égal à l'idéal engendré par les modules de Cauchy. Cela fonctionne avec une belle formule :

Fait 1.4 *Introduisons une nouvelle variable T.*

1. *Dans $\mathbf{A}[X_1, \ldots, X_n, T]$, on a*

$$\begin{aligned}
f(T) &= f_1(X_1) + (T - X_1)f_2(X_1, X_2) + (T - X_1)(T - X_2)f_3(X_1, X_2, X_3) + \cdots\\
&\quad + (T - X_1) \cdots (T - X_{n-1})f_n(X_1, \ldots, X_n) + (T - X_1) \cdots (T - X_n)
\end{aligned} \tag{1}$$

2. *Dans le sous $\mathbf{A}[X_1, \ldots, X_n]$-module de $\mathbf{A}[X_1, \ldots, X_n, T]$ formé par les polynomes de degré $\leq n$ en T, le polynome $f(T) - (T - X_1) \cdots (T - X_n)$ possède deux expressions différentes :*
   - *D'une part, sur la base $1, T, T^2, \ldots, T^n$ il a pour coordonnées $(-1)^n(a_n - \alpha_n), \ldots, (a_2 - \alpha_2), -(a_1 - \alpha_1), 0$*
   - *D'autre part, sur la base $1, (T - X_1), (T - X_1)(T - X_2), \ldots, (T - X_1) \cdots (T - X_n)$ il a pour coordonnées $f_1, f_2, \ldots, f_n, 0$*
3. *En conséquence sur l'anneau $\mathbf{A}[X_1, \ldots, X_n]$, chacun des deux vecteurs*

$$((-1)^n(a_n - \alpha_n), \ldots, (a_2 - \alpha_2), -(a_1 - \alpha_1)) \qquad \text{et} \qquad (f_1, \ldots, f_{n-1}, f_n)$$

s'exprime en fonction de l'autre au moyen d'une matrice unipotente (triangulaire avec des 1 sur la diagonale).

Preuve Il suffit de prouver le point 1. On a

$$f(T) = f(X_1) + (T - X_1)f_2(X_1, T)$$

par définition de $f_1 = f$ et f_2. De même

$$f_2(X_1, T) = f_2(X_1, X_2) + (T - X_2)f_3(X_1, X_2, T)$$

par définition de f_3. Donc

$$f(T) = f(X_1) + (T - X_1)f_2(X_1, X_2) + (T - X_1)(T - X_2)f_3(X_1, X_2, T)$$

On continue jusqu'à

$$f_{n-1}(X_1, \ldots, X_{n-2}, T) = f_{n-1}(X_1, \ldots, X_{n-2}, X_{n-1}) + (T - X_{n-1})f_n(X_1, \ldots, X_{n-1}, T)$$

Ce qui donne

$$\begin{aligned} f(T) \;=\; & f_1(X_1) + (T - X_1)f_2(X_1, X_2) + (T - X_1)(T - X_2)f_3(X_1, X_2, X_3) + \cdots \\ & + (T - X_1)\cdots(T - X_{n-1})f_n(X_1, \ldots, X_{n-1}, T) \end{aligned}$$

Enfin $f_n(X_1, \ldots, X_{n-1}, T)$ est unitaire de degré 1 en T donc

$$f_n(X_1, \ldots, X_{n-1}, T) = f_n(X_1, \ldots, X_{n-1}, X_n) + (T - X_n).$$

□

Notez que ceci prouve en particulier que $f_n = \alpha_1 - a_1$.

Lemme 1.5 *Pour tout élément $z \in \mathbf{B}$ on a $\mathrm{C}_{\mathbf{B}/\mathbf{A}}(z)(T) = \mathrm{C}_{\mathrm{S}_n}(z)(T)$. En particulier $\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(z) = \mathrm{Tr}_{\mathrm{S}_n}(z)$ et $\mathrm{N}_{\mathbf{B}/\mathbf{A}}(z) = \mathrm{N}_{\mathrm{S}_n}(z)$.*

Preuve Puisque le polynome caractéristique est la norme de $T - z$ il suffit de montrer l'égalité des deux « normes » : $\mathrm{N}_{\mathbf{B}/\mathbf{A}}(z) = \prod_{\sigma\in\mathrm{S}_n} \sigma(z)$. Écrivons $\mathrm{N}_{\mathrm{S}_n}(z)$ sur la base canonique $\mathcal{B}(f)$, c'est clairement un élément de $\mathbf{A}$. Si on prend pour coefficients de f des indéterminées a_i, pour coordonnées de z sur la base $\mathcal{B}(f)$ d'autres indéterminées et pour $\mathbf{A}$ l'anneau librement engendré par ces indéterminées on voit qu'il s'agit de démontrer une identité algébrique, c'est-à-dire une égalité entre deux éléments d'un anneau de polynomes à coefficients dans $\mathbb{Z}$. Notons N pour $\mathrm{N}_{\mathbf{B}/\mathbf{A}}$. Comme $\mathrm{N}(z) = \mathrm{N}(\sigma(z))$ pour tout $\sigma \in \mathrm{S}_n$, on obtient $\mathrm{N}(\prod_{\sigma\in\mathrm{S}_n} \sigma(z)) = \mathrm{N}(z)^{n!}$. Puisque $\mathrm{N}_{\mathrm{S}_n}(z) \in \mathbf{A}$, $\mathrm{N}(\mathrm{N}_{\mathrm{S}_n}(z)) = (\mathrm{N}_{\mathrm{S}_n}(z))^{n!}$. Ainsi $\mathrm{N}(z)$ et $\mathrm{N}_{\mathrm{S}_n}(z)$ sont deux polynomes en les indéterminées qui sont égaux après avoir été élevés à la puissance $n!$. Puisqu'on est dans un anneau factoriel, on doit avoir $\mathrm{N}_{\mathrm{S}_n}(z) = c\,\mathrm{N}(z)$ avec $c \in \mathbb{Z}$ et $c^{n!} = 1$. Enfin, puisque toute situation particulière est obtenue comme spécialisation de la situation générale (avec des coefficients indéterminés), pour connaître c on peut spécialiser z en 1 : $c = 1$. □

2 Idempotents galoisiens

Dans la suite nous notons $\mathbb{B}(\mathbf{C})$ l'algèbre de Boole des idempotents d'un anneau $\mathbf{C}$. Les opérations sont $u \wedge v := u\,v$, $u \vee v := u + v - u\,v$, $u \oplus v := u + v - 2u\,v = (u - v)^2$, $\neg u := 1 - u = 1 \oplus u$. Et la relation dordre partiel est $u \leq v \iff u \wedge v = u \iff u \vee v = v$.

Dans une algèbre de Boole un élément non nul minimal est parfois appelé un *atome*. Dans le cas d'un idempotent dans un anneau on parle d'*idempotent indécomposable*.

Rappelons qu'un automorphisme σ d'un anneau $\mathbf{C}$ est dit *séparant* s'il existe $x_1, \ldots x_k, a_1, \ldots, a_k \in \mathbf{C}$ tels que $1 = \sum_{i=1}^{k} a_i(x_i - \sigma(x_i))$ et qu'un groupe G d'automorphismes de $\mathbf{C}$ est dit *séparant* si les éléments $\neq \mathrm{Id}_{\mathbf{C}}$ de G sont séparants. Une *algèbre galoisienne* est par définition un triplet $(\mathbf{A}, \mathbf{C}, G)$ où G est un groupe séparant d'automorphismes de $\mathbf{C}$ et $\mathbf{A} = \mathrm{Fix}(G)$ est le sous-anneau des points fixes de G (cf. [5]).

Nous utiliserons les notations suivantes lorsqu'un groupe G opère sur un ensemble E. Pour $x \in E$, $\mathrm{St}(x)$ désigne le stabilisateur de x, pour $F \subset E$, $\mathrm{Stp}(F)$ désigne le stabilisateur point par point de F. Et si $H \subset G$, $\mathrm{Fix}(H) = E^H$ désigne la partie de E formée des éléments fixés par tous les $\sigma \in H$.

Nous donnons maintenant une définition qui permet d'insérer l'algèbre de décomposition universelle dans un cadre un peu plus général et utile.

Définition 2.1 (algèbre prégaloisienne)
Une algèbre prégaloisienne est donnée par un triplet $(\mathbf{A}, \mathbf{C}, G)$ *où*

1. $\mathbf{C}$ *est une* $\mathbf{A}$*-algèbre avec* $\mathbf{A} \subset \mathbf{C}$*,* $\mathbf{A}$ *facteur direct dans* $\mathbf{C}$*,*
2. G *est un groupe fini de* $\mathbf{A}$*-automorphismes de* $\mathbf{C}$*,*
3. $\mathbf{C}$ *est un* $\mathbf{A}$*-module projectif de rang constant* $|G|$*,*
4. *pour tout* $z \in \mathbf{C}$*,* $\mathrm{C}_{\mathbf{C}/\mathbf{A}}(z) = \mathrm{C}_G(z)$*.*

Par exemple $(\mathbf{A}, \mathbf{B}, \mathrm{S}_n)$ (avec toujours $\mathbf{B} = \mathrm{Adu}_{\mathbf{A},f}$) est une algèbre prégaloisienne.

NB : La notion d'algèbre prégaloisienne est un peu moins contraignante que la notion plus usuelle d'algèbre galoisienne.

Définition 2.2 *Dans une algèbre prégaloisienne* $(\mathbf{A}, \mathbf{C}, G)$ *un idempotent* e *de* $\mathbf{C}$ *est dit* galoisien *si son orbite sous* G *est un sfio.*

Théorème 2.3 (théorème de structure, 1)
Soit une algèbre prégaloisienne $(\mathbf{A}, \mathbf{C}, G)$*,* e *un idempotent galoisien de* $\mathbf{C}$*, et* $\{e_1, \ldots, e_m\}$ *son orbite sous* G*. Soit* H *le stabilisateur de* $e = e_1$ *et* $r = |H|$*, de sorte que* $rm = |G|$*. Posons* $\mathbf{C}_i = \mathbf{C}/\langle 1 - e_i \rangle \simeq e_i\mathbf{C}$ $(1 \leq i \leq m)$*. Soit enfin* $\pi : \mathbf{C} \to \mathbf{C}_1$ *la projection canonique.*

1. *Les* $\mathbf{C}_i$ *sont des* $\mathbf{A}$*-algèbres deux à deux isomorphes, et* $\mathbf{C} \simeq \mathbf{C}_1^m$ *(comme* $\mathbf{A}$*-algèbres).*
2. *L'algèbre* $\mathbf{C}_1$ *est un* $\mathbf{A}$*-module projectif de rang constant* $r = |H|$*. La restriction de* π *à* $\mathbf{A}$*, et même à* $\mathbf{C}^G$*, est injective. Et* $\mathbf{A}$ *(identifié à son image dans* $\mathbf{C}_1$*) est facteur direct dans* $\mathbf{C}_1$*.*
3. *Le groupe* H *opère sur* $\mathbf{C}_1$ *et* $\mathbf{C}_1^H$ *est canoniquement isomorphe à* $\mathbf{C}^G$ *: plus précisément* $\mathbf{C}_1^H = \pi(\mathbf{C}^H) = \pi(\mathbf{C}^G)$*.*
4. *Pour tout* $z \in \mathbf{C}_1$*,* $\mathrm{C}_{\mathbf{C}_1/\mathbf{A}}(z)(T) = \mathrm{C}_H(z)(T)$*.*
5. $(\mathbf{A}, \mathbf{C}_1, H)$ *est une algèbre prégaloisienne, on dira que c'est un* quotient de Galois *de* $(\mathbf{A}, \mathbf{C}, G)$*.*
6. *Soit* g_1 *un idempotent galoisien de* $(\mathbf{A}, \mathbf{C}_1, H)$*,* K *son stabilisateur dans* H*,* $g' \in e_1\mathbf{C}$ *tel que* $\pi(g') = g_1$*. Alors* g' *est un idempotent galoisien de* $(\mathbf{A}, \mathbf{C}, G)$*, son stabilisateur est* K*, et on a un isomorphisme canonique* $\mathbf{C}_1/\langle 1 - g_1 \rangle \simeq \mathbf{C}/\langle 1 - g' \rangle$*.*

Preuve Le point 1 est évident. La première affirmation du point 2 en est une conséquence immédiate. Soit $\tau_1 = \mathrm{Id}, \tau_2, \ldots, \tau_m$ un système de représentants pour G/H, avec $\tau_i(e_1) = e_i$. Montrons que la restriction de π à $\mathbf{C}^G$ est injective : si $a \in \mathbf{C}^G$ et $e_1 a = 0$ alors en transformant par les τ_j, tous les $e_j a$ sont nuls, et donc aussi leur somme, égale à a. Montrons que $\pi(\mathbf{A})$ est facteur direct dans $\mathbf{C}_1$. Soit $\lambda : \mathbf{C}_1 \to e_1\mathbf{C}$ l'isomorphisme réciproque de la restriction de π à $e_1\mathbf{C}$. Il s'agit d'un isomorphisme de $\mathbf{A}$-algèbres, e_1 étant l'élément neutre pour la multiplication dans $e_1\mathbf{C}$. Soit $\varphi : \mathbf{C} \to \mathbf{A}$ une forme $\mathbf{A}$-linéaire vérifiant $\varphi(1) = 1$. On définit $\psi : \mathbf{C}_1 \to \pi(\mathbf{A})$ par $\psi(y) = \pi(\varphi(x + \tau_2(x) + \cdots + \tau_m(x)))$ où $x = \lambda(y)$. On a bien que ψ est une forme linéaire vérifiant $\psi(1) = 1$ donc $\mathbf{C}_1 = \pi(\mathbf{A}) \oplus \mathrm{Ker}\,\psi$.
Voyons le point 3. Montrons d'abord $\mathbf{C}_1^H = \pi(\mathbf{C}^H)$. Soit $u \in \mathbf{C}$ tel que $\pi(u) = z \in \mathbf{C}_1^H$. Puisque $z \in \mathbf{C}_1^H$, pour tout $\sigma \in H$, $\sigma(u) \equiv u \bmod \langle 1 - e_1 \rangle$, ce qui signifie, $e_1\sigma(u) = e_1 u$. Comme $\sigma(e_1) = e_1$ et $\pi(e_1) = 1_{\mathbf{C}_1}$ on obtient avec $y = e_1 u$: $\pi(y) = z$ et pour tout $\sigma \in H$, $\sigma(y) = y$ c'est-à-dire $z \in \pi(\mathbf{C}^H)$. Montrons maintenant que $z \in \pi(\mathbf{C}^G)$. On pose $v = \sum_i \tau_i(y) = \sum_i \tau_i(e_1 y) = \sum_i e_i\tau_i(y)$. On a $\pi(e_i) = \delta_{1i}$ et donc $\pi(v) = \pi(y)$. Montrons que v est fixe par G. Si $\sigma \in G$, $\sigma(v) = \sum_i \sigma(e_i\tau_i(y))$. Fixons i et posons $\sigma(e_i) = e_j$. Notre but est de montrer que $\sigma(\tau_i(y)) = \tau_j(y)$, c'est-à-dire que $\tau_j^{-1}\sigma\tau_i$ fixe y. Or cela résulte de $y \in \mathbf{C}^H$ et $\tau_j^{-1}\sigma\tau_i \in H$ puisque $\tau_j^{-1}\sigma\tau_i(e_1) = e_1$.
Voyons le point 4. Soit u tel que $\pi(u) = z$ et $y = e_1 u$. On a $\pi_i(y) = 0$ pour $i \neq 1$ et $\pi(y) = z$. Dans

la décomposition $\mathbf{C} = e_1\mathbf{C} \oplus \cdots \oplus e_m\mathbf{C}$, y s'ecrit donc $(y, 0, \ldots, 0)$ et $T - y$ s'écrit $(T - y, T, \ldots, T)$. Cela donne $\mathrm{C}_{\mathbf{C}/\mathbf{A}}(y)(T) = T^p\,\mathrm{C}_{\mathbf{C}_1/\mathbf{A}}(z)$ avec $p = |G| - |H|$. En considérant $\sigma(y)$ pour un $\sigma \in G$ arbitraire on peut écrire $\sigma = \tau_i\lambda$ pour un certain i et un élément λ de H. Ceci permet de voir que la composante dans $e_1\mathbf{C}$ de $\mathrm{C}_G(y)(T)$ n'est autre que $T^p\,\mathrm{C}_H(z)(T)$ (qu'on remonte de $\mathbf{C}_1[T]$ dans $e_1\mathbf{C}[T]$). Par raison de symétrie il en sera de même pour les autres composantes, c'est-à-dire qu'on a $\mathrm{C}_G(y)(T) = T^p\,\mathrm{C}_H(z)(T)$.
Le point 5 est une synthèse des points précédents.
Voyons le point 6. En tenant compte du fait que la restriction de π à $e_1\mathbf{C}$ est un isomorphisme on a $g'^2 = g' = g'e_1$. De même pour $\sigma \in H$ on a : $\sigma(g') = g'$ si $\sigma \in K$, ou $g'\sigma(g') = 0$ si $\sigma \notin K$. Enfin pour $\sigma \in G \setminus H$, $e_1\sigma(e1) = 0$ et donc $g'\sigma(g') = 0$. Ceci montre que g' est un idempotent galoisien de $\mathbf{B}$ avec pour stabilisateur K. L'isomorphisme canonique est immédiat. □

Il est souhaitable qu'on puisse tester l'égalité de deux idempotents dans l'algèbre de décomposition universelle $\mathbf{B}$, ce qui revient à savoir tester $e = 0$ pour un idempotent arbitraire de $\mathbf{B}$. En fait $e\mathbf{B}$ est un $\mathbf{A}$-module projectif de type fini et $e = 0$ si et seulement si son « polynome rang » (c'est-à-dire le déterminant de la multiplication par T dans le $\mathbf{A}$-module $e\mathbf{B}$) est égal à 1. Il est connu que le polynome rang d'un $\mathbf{A}$-module projectif de type fini a pour coefficients un sfio de $\mathbf{A}$. En outre ce polynome peut être calculé explicitement. Donc on peut tester l'égalité de deux idempotents dans $\mathbf{B}$ si et seulement si on peut tester l'égalité de deux idempotents dans $\mathbf{A}$. L'argument ci-dessus fonctionne dans un cadre un peu plus général et on obtient :

Fait 2.4 *L'algèbre de Boole* $\mathbb{B}(\mathbf{B})$ *est discrète si et seulement si* $\mathbb{B}(\mathbf{A})$ *est discrète. Plus généralement si* $\mathbf{A} \subset \mathbf{C}$ *et* $\mathbf{C}$ *est un* $\mathbf{A}$*-module projectif de type fini,* $\mathbb{B}(\mathbf{C})$ *est discrète si et seulement si* $\mathbb{B}(\mathbf{A})$ *est discrète.*

Fait 2.5 *Si* $(\mathbf{A}, \mathbf{C}, G)$ *est une algèbre prégaloisienne, un idempotent de* $\mathbf{C}$ *fixé par* G *est un élément de* $\mathbf{A}$*.*

Preuve Soit e un idempotent de $\mathbf{C}$. Alors $\mathrm{C}_G(e) = (T - e)^{|G|}$ est dans $\mathbf{A}[T]$ donc son coefficient constant, qui est égal à $\pm e$ est dans $\mathbf{A}$. □

Définition 2.6 *Un anneau* $\mathbf{A}$ *est dit* connexe *si ses seuls idempotents sont* 0 *et* 1*.*

Commentaire. En mathématiques classiques il revient au même de dire que le spectre de Zariski de $\mathbf{A}$ est connexe.

Fait 2.7 *Soit* $(\mathbf{A}, \mathbf{C}, G)$ *une algèbre prégaloisienne avec* $\mathbf{A}$ *connexe et non trivial :*

1. 0 *et* 1 *sont les seuls idempotents de* $\mathbf{C}$ *fixés par* G*,*
2. $\mathbb{B}(\mathbf{C})$ *est discrète,*
3. *tout atome de* $\mathbb{B}(\mathbf{C})$ *est un idempotent galoisien,*
4. *deux atomes sont conjugués sous* G*.*

Preuve 1 et 2 résultent clairement des faits 2.5 et 2.4.
Pour le point 3 : Si e est un atome et $\sigma(e) \neq e$ alors $e\sigma(e) = 0$ car c'est un multiple strict de e. De même deux éléments de l'orbite de e sont orthogonaux, donc la somme de l'orbite de e est un idempotent non nul fixé par G : il est égal à 1.
Pour le point 4 : Si e' est un autre atome, il est égal la somme des e_ie', où e_i parcourt l'orbite de e. Et comme les e_i sont minimaux, chacun des e_ie' est nul ou égal à e_i. □

3 Éléments galoisiens dans une algèbre de Boole

Le fait suivant constitue un raffinement constructif de la théorie des algèbres de Boole finies.

Fait 3.1 *Soit* C *une algèbre de Boole. Les propriétés suivantes sont équivalentes :*

1. *C est finie.*
2. *C est discrète et de type fini.*
3. *1_C est une somme finie d'atomes.*

Dans un tel cas C est isomorphe à l'algèbre de Boole $\mathcal{P}(S)$ des parties finies de l'ensemble S des atomes.

En particulier dans le contexte des anneaux commutatifs $\mathbb{B}(\mathbf{C})$ est finie si et seulement si $1_{\mathbf{C}}$ est une somme d'idempotents indécomposables orthogonaux.

Commentaire. Une situation fréquente est celle d'une algèbre de Boole C *bornée* (on a une majoration du nombre de ses éléments) et discrète, mais où on ne connaît pas d'atome de manière sûre. Les idéaux de type fini de C, tous principaux, s'identifient aux éléments de C, donc C s'identifie à son propre treillis de Zariski([1]) $\operatorname{Zar} C$. Par ailleurs, en mathématiques classiques les atomes sont en bijection avec les idéaux premiers (tous maximaux) de C via $e \mapsto \langle 1-e\rangle$. Ainsi l'ensemble des atomes de C (supposée bornée) s'identifie à $\mathsf{Spec}\, C$. On retrouve donc dans ce cas particulier le fait général suivant : le treillis de Zariski est la version constructive, maniable et « sans point » du spectre de Zariski, espace topologique dont les points peuvent s'avérer inaccessibles d'un point de vue constructif. Mais cette situation, bien que familière, est peut être plus troublante dans le cas d'un espace topologique discret et borné. Il s'agit typiquement d'un espace compact dont on n'a pas une bonne description via un sous ensemble énumérable dense, donc qui n'entre pas dans le cadre des espaces métriques compacts à la Bishop [2].

Définition 3.2 *Si G est un groupe fini qui opère sur une algèbre de Boole C, un élément e de C est dit* galoisien *(pour G) si son orbite sous G est un sfio : les éléments de l'orbite sont deux à deux orthogonaux et leur somme est égale à 1.*

Fait 3.3 *Soit G un groupe fini opérant sur une algèbre de Boole C discrète, $e \neq 0$ dans C, et $\{e_1, \dots, e_k\}$ l'orbite de e sous G. On suppose que 1 et 0 sont les seuls éléments fixés par G. Les propriétés suivantes sont équivalentes :*

1. *L'élément e est galoisien.*
2. *Pour tout $i > 1$, $e_1 e_i = 0$.*
3. *Pour tout $\sigma \in G$, $e\sigma(e) = e$ ou 0.*
4. *Pour tous $i \neq j \in \{1, \dots, k\}$, $e_i e_j = 0$.*

Les hypothèses sont vérifiées par exemple si $C = \mathbb{B}(\mathbf{B})$, $G = \mathrm{S}_n$ et $\mathbf{A}$ est connexe.

Preuve Le point 1 implique clairement les autres. Les points 2 et 4 sont facilement équivalents et impliquent le point 3. Le point 3 signifie que pour tout σ, $\sigma(e) \geq e$ ou $\sigma(e)e = 0$. Si on a $\sigma(e) \geq e$ pour un certain σ alors on a $e \leq \sigma(e) \leq \sigma^2(e) \leq \sigma^3(e) \leq \cdots$ ce qui donne $e = \sigma(e)$ en considérant $\sigma^k = 1_G$. Donc 3 implique 2. Enfin si le point 4 est vérifié, la somme de l'orbite est un élément > 0 fixé par G donc égal à 1. □

Théorème 3.4 (théorème de structure, 2)
Soit G un groupe fini opérant sur une algèbre de Boole C discrète et non triviale. On suppose que 1 et 0 sont les seuls éléments fixés par G (par exemple, $C = \mathbb{B}(\mathbf{C})$, $(\mathbf{A}, \mathbf{C}, G)$ est une algèbre prégaloisienne et $\mathbf{A}$ est connexe).

1. *Pour toute famille finie d'éléments de C il existe un élément galoisien e_1 (notons $(e_1, \dots, e_k)$ son orbite) et tel que chaque idempotent e de la famille initiale vérifie $e = \sum \{e_i \mid 1 \leq i \leq k,\ e_i e \neq 0\}$.*
2. *L'algèbre de Boole C ne peut avoir plus que $2^{|G|}$ éléments.*
3. *Si e et h sont des éléments galoisiens avec $e < h$ (cad $he = e$ et $h \neq e$) si E est le stabilisateur de e et H le stabilisateur de h alors $h = \sum_{\sigma \in H/E} \sigma(e)$.*

[1] Rappelons que pour un anneau commutatif $\mathbf{A}$, $\operatorname{Zar}\mathbf{A}$ est l'ensemble des radicaux d'idéaux de type fini de $\mathbf{A}$. C'est un treillis distributif. En mathématiques classiques, $\operatorname{Zar}\mathbf{A}$ s'identifie au treillis des ouverts quasi-compacts de $\mathsf{Spec}\,\mathbf{A}$.

4. C est finie si et seulement si il existe un atome e. Dans ce cas e est galoisien, l'orbite de e est l'ensemble des atomes, G opère sur cette orbite comme sur G/E, et sur C comme sur $\mathcal{P}(G/E)$([2]).

Preuve Voyons le point 1. On considère la sous-algèbre de Boole $C' \subseteq C$ engendrée par les orbites des éléments de la famille finie donnée. C' est de type fini et discrète donc finie. En conséquence ses éléments minimaux non nuls forment un ensemble fini $S = \{e_1, \dots, e_k\}$ et C' est isomorphe à l'algèbre de Boole des parties finies de S : $C' = \{\sum_{i\in F} e_i | F \in \mathcal{P}(\{1, \dots, k\})\}$. Clairement G opère sur C'. Pour $\sigma \in \mathrm{S}_n$, $\sigma(e_1)$ est une somme de certains e_i, mais il ne peut y avoir deux termes dans la somme, car alors en transformant l'un de ces termes par σ^{-1} on aurait un élément non nul $< e_1$ dans C'. Donc $(e_1, \dots, e_k)$ est un sfio et e_1 est galoisien.
Le point 2 est conséquence du 1.
Voyons le point 3. Si $\sigma \in H$, alors $\sigma(h) = h$ donc $\sigma(e)h = \sigma(eh) = \sigma(e) \neq 0$. Si $\sigma \notin H$, alors $h\sigma(h) = 0$ donc $\sigma(e)h = \sigma(eh)h = \sigma(e)\sigma(h)h = 0$. Le point 1 donne $h = \sum_{\sigma\in H/E} \sigma(e)$.
Pour le point 4, on raisonne comme pour le fait 2.7. □

Sous les hypothèses du théorème précédent on peut calculer un élément galoisien e_1 qui engendre la même algèbre de Boole que l'orbite de e au moyen de l'algorithme suivant. On pourra penser au cas $C = \mathbb{B}(\mathbf{B})$, $G = \mathrm{S}_n$ et $\mathbf{A}$ connexe, ou plus généralement $C = \mathbb{B}(\mathbf{C})$, $(\mathbf{A}, \mathbf{C}, G)$ est une algèbre prégaloisienne et $\mathbf{A}$ est connexe. En outre on peut également calculer le stabilisateur de e_1 (la *nouvelle approximation du groupe de Galois*) « sans sortir du groupe » :

Algorithme 3.5 ***Calcul d'un élément galoisien et de son stabilisateur.***
Entrée : e : élément non nul d'une algèbre de Boole C ; G : groupe fini d'automorphismes de C ; $S = \mathrm{St}(e)$ (sous groupe stabilisateur de e).
On suppose que 0 et 1 sont les seuls points fixes pour l'action de G sur C.
Sortie : e_1 : élément galoisien correspondant ; H : le sous groupe stabilisateur de e_1.
Variables locales : h : dans C ; σ : dans G ; L : liste d'éléments de G.
Début
$e_1 \leftarrow e$; $L \leftarrow [\,]$;
pour σ **dans** G/S **faire**
G/S désigne un système de représentants des classes à gauche modulo S
$h \leftarrow e_1\sigma(e)$;
si $h \neq 0$ **alors** $e_1 \leftarrow h$; $L \leftarrow L \bullet [\sigma]$ **fin si** ;
fin pour
$H \leftarrow$ le sous-groupe de G formé par les α qui vérifient : $\forall \sigma \in L$, $\alpha\sigma \in \bigcup_{\tau\in L} \tau S$.
Fin.

Preuve Nous avons noté G/S un système de représentants des classes à gauche modulo S. Écrivons $e_1 = e\sigma_2(e)\cdots\sigma_r(e)$ où les σ_i sont tous les σ qui ont passé avec succès le test $h \neq 0$ dans l'algorithme (et $\sigma_1 = \mathrm{Id}$). Nous voulons montrer que e_1 est un élément minimal dans C', ce qui revient à dire que pour tout $\sigma \in G/S$ on a $e_1\sigma(e) = e_1$ ou 0 (puisque C' est engendrée par les $\tau(e)$). Or σ a été testé par l'algorithme, donc ou bien σ est l'un des σ_i auquel cas $e_1\sigma(e) = e_1$ ou bien $g\sigma(e) = 0$ pour un idempotent g qui divise e_1 et a fortiori $e_1\sigma(e) = 0$.
Montrons que le stabilisateur H de e_1 vérifie bien la condition requise. On a $e_1 = \prod_{\tau\in L} \tau(e)$, et pour $\sigma \in G$ on a les équivalences :

$$\sigma \in \bigcup_{\tau\in L} \tau S \;\Leftrightarrow\; e_1\sigma(e) = e_1 \;\Leftrightarrow\; e_1 \leq \sigma(e), \qquad \text{et} \qquad \sigma \notin \bigcup_{\tau\in L} \tau S \;\Leftrightarrow\; e_1\sigma(e) = 0.$$

Pour $\alpha \in G$ on a $\alpha(e_1) = \prod_{\tau\in L} \alpha(\tau(e))$. C'est un élément de l'orbite de e_1, il est égal à e_1 si et seulement si $e_1 \leq \alpha(e_1)$, si et seulement si $e_1 \leq \alpha(\sigma(e))$ pour chaque σ in L. Enfin, pour un σ arbitraire dans G, $e_1 \leq \alpha(\sigma(e))$ si et seulement si $\alpha\sigma$ est dans $\bigcup_{\tau\in L} \tau S$. □

[2] Ici, pour que l'affirmation soit valide d'un point de vue constructif, $\mathcal{P}(G/E)$ dénote l'ensemble des parties *finies* de G/E.

On notera que l'élément e_1 obtenu comme résultat du calcul dépend de l'ordre dans lequel est énuméré l'ensemble fini G/S et qu'il n'y a pas d'ordre naturel (intrinsèque) sur cet ensemble.

Exemple. On peut se demander s'il existe un rapport entre le stabilisateur S de e et le stabilisateur H de l'élément galoisien e_1 associé à e. Voici un exemple qui montre qu'il n'y a pas de rapport étroit, avec $G = \mathrm{S}_6$ opérant sur l'algèbre de décomposition universelle du polynome $f(T) = (T+1)^6 - 4(T+1)^3 + 7$ et e l'idempotent que l'on calcule partir de l'élément $x_1 + x_2$ qui n'est ni nul ni inversible (cf. théorème 6.7). On trouve $\mathrm{St}(e) = S = \langle (12), (34), (3456) \rangle \simeq \mathrm{S}_2 \times \mathrm{S}_4$ avec $|S| = 48$, et $\mathrm{St}(e_1) = H = \langle (123456), (26) \rangle = (\langle (13), (135) \rangle \times \langle (24), (246) \rangle) \rtimes \langle (12)(36)(45) \rangle \simeq (\mathrm{S}_3 \times \mathrm{S}_3) \rtimes \mathrm{S}_2$ avec $|H| = 72$, et $S \cap H = \langle (46), (35), (12)(36)(45) \rangle$ diedral d'ordre 8.
En bref, H (ni même la classe de conjugaison de H dans G) ne peut être calculé à partir de S seulement car la liste L de classes à gauche sélectionnée par l'algorithme ne dépend pas seulement du sous-groupe S de G mais aussi de la façon dont G opère sur C.

4 Séparabilité, points fixes

Lemme 4.1 *Soit* $\mathbf{C}$ *une* $\mathbf{A}$*-algèbre qui est un module projectif de rang constant* $k \geq 1$ *(par exemple une algèbre prégaloisienne ou* $\mathbf{C} = \mathbf{B}$*).*

1. *Un élément* x *de* $\mathbf{C}$ *est inversible si et seulement si* $\mathrm{N}_{\mathbf{C}/\mathbf{A}}(x)$ *est inversible dans* $\mathbf{A}$*.*
2. *Un élément* x *de* $\mathbf{A}$ *est inversible dans* $\mathbf{C}$ *si et seulement si il est inversible dans* $\mathbf{A}$*.*
3. *Un élément* x *de* $\mathbf{C}$ *est régulier si et seulement si* $\mathrm{N}_{\mathbf{C}/\mathbf{A}}(x)$ *est régulier dans* $\mathbf{A}$*.*
4. *Un élément* x *de* $\mathbf{A}$ *est régulier dans* $\mathbf{C}$ *si et seulement si il est régulier dans* $\mathbf{A}$*.*

Preuve Le point 1 : dans un module projectif de type fini un endomorphisme (ici la multiplication par x) est bijectif si et seulement si son déterminant est inversible.
Le point 3 : dans un module projectif de type fini un endomorphisme est injectif si et seulement si son déterminant est régulier.
Les points 2 et 4 se déduisent de 1 et 3 parce que $\mathrm{N}_{\mathbf{C}/\mathbf{A}}(x) = x^k$. □

Lemme 4.2 *Soit* J *le jacobien du système de* n *équations à* n *inconnues définissant l'algèbre de décomposition universelle* $\mathbf{B} = \mathrm{Adu}_{\mathbf{A},f}$*.*

1. *On a* $J = \prod_{1 \leq i < j \leq n} (x_i - x_j)$ *dans* $\mathbf{B}$*.*
2. *On a* $J^2 = \mathrm{disc}\, f \in \mathbf{A}$*.*
3. *En particulier les propriétés suivantes sont équivalentes :*
   (a) $\mathrm{disc}\, f$ *est inversible (resp. régulier) dans* $\mathbf{A}$*.*
   (b) J *est inversible (resp. régulier) dans* $\mathbf{B}$*.*
   (c) *Les* $x_i - x_j$ *sont inversibles (resp. réguliers) dans* $\mathbf{B}$*.*
   (d) $x_1 - x_2$ *est inversible (resp. régulier) dans* $\mathbf{B}$*.*
   (e) $\Omega_{\mathbf{B}/\mathbf{A}} = 0$ *(resp.* $\Omega_{\mathbf{B}/\mathbf{A}}$ *est un* $\mathbf{B}$*-module « de torsion », i.e. annulé par un élément régulier).*

Preuve Le point 1 est facile par récurrence sur n, avec le signe exact si on considére le système qui nous a servi pour la définition de l'algèbre de décomposition universelle. Voici par exemple le calcul

pour $n = 4$

$$\begin{aligned} J &= \begin{vmatrix} 1 & 1 & 1 & 1 \\ \sum_{i\neq 1} x_i & \sum_{i\neq 2} x_i & \sum_{i\neq 3} x_i & \sum_{i\neq 4} x_i \\ \sum_{i,j\neq 1} x_i x_j & \sum_{i,j\neq 2} x_i x_j & \sum_{i,j\neq 3} x_i x_j & \sum_{i,j\neq 4} x_i x_j \\ x_2x_3x_4 & x_1x_3x_4 & x_1x_2x_4 & x_1x_2x_3 \end{vmatrix} \\ &= \begin{vmatrix} 1 & 0 & 0 & 0 \\ \sum_{i\neq 1} x_i & x_1 - x_2 & x_1 - x_3 & x_1 - x_4 \\ \sum_{i,j\neq 1} x_i x_j & (x_1 - x_2)\sum_{i\neq 1,2} x_i & (x_1 - x_3)\sum_{i\neq 1,3} x_i & (x_1 - x_4)\sum_{i\neq 1,4} x_i \\ x_2x_3x_4 & (x_1 - x_2)x_3x_4 & (x_1 - x_3)x_2x_4 & (x_1 - x_4)x_2x_3 \end{vmatrix} \\ &= (x_1 - x_2)(x_1 - x_3)(x_1 - x_4) \begin{vmatrix} 1 & 1 & 1 \\ x_3 + x_4 & x_2 + x_4 & x_2 + x_3 \\ x_3x_4 & x_2x_4 & x_2x_3 \end{vmatrix} \end{aligned}$$

etc...

Le point 2 est une conséquence immédiate du point 1, et on en déduit l'équivalence des points (a) à (d) dans 3, en tenant compte du lemme 4.1.

Pour le point (e) rappelons que $\Omega_{\mathbf{B}/\mathbf{A}}$ est un $\mathbf{B}$-module isomorphe au conoyau de la matrice jacobienne, ce qui implique que $\mathrm{Ann}(\Omega_{\mathbf{B}/\mathbf{A}})$ et $J\mathbf{B}$ ont même nilradical. Enfin J est régulier (resp. inversible) si et seulement si $\sqrt{\langle J\rangle}$ contient un élément régulier (resp. contient 1). □

Rappelons le fait suivant concernant le résultant de deux polynomes lorsque l'un d'entre eux est unitaire.

Fait 4.3 *Si $g, h \in \mathbf{A}[T]$ et g unitaire de degré n, $\mathrm{Res}_T(g, h) = R$ est bien défini (il n'y a pas besoin de connaître le degré de h) et*

$$\langle R^n\rangle \subseteq \langle g, h\rangle \cap \mathbf{A} \subseteq \langle R\rangle .$$

En particulier

- $\langle g, h\rangle = \langle 1\rangle$ *si et seulement si R est inversible.*
- $\mathrm{Ann}_{\mathbf{A}[T]}(\langle g, h\rangle) = 0$ *si et seulement si* $\mathrm{Ann}_{\mathbf{A}}(R) = 0$

En particulier $\mathrm{Ann}_{\mathbf{A}[T]}(\langle f(T), f'(T)\rangle) = 0$ si et seulement si $\mathrm{disc}\, f$ est un élément régulier de $\mathbf{A}$.

Nous notons $\mathrm{di}(f) = \prod_{1\leq i<j\leq n}(x_i + x_j) \in \mathbf{A}$.

Il est clair que $\mathrm{di}(f)$ est congru modulo 2 à $\prod_{1\leq i<j\leq n}(x_i - x_j)$ et donc $\langle 2, \mathrm{di}(f)^2\rangle = \langle 2, \mathrm{disc}(f)\rangle$.

Théorème 4.4 *Si* $\mathrm{Ann}_{\mathbf{A}}(\langle 2, \mathrm{di}(f)\rangle) = 0$ *et a fortiori si* $\mathrm{Ann}_{\mathbf{A}}(\langle 2, \mathrm{disc}(f)\rangle) = 0$ *on a* $\mathrm{Fix}(\mathrm{S}_n) = \mathbf{A}$.

Preuve Puisque $\langle 2, \mathrm{di}(f)^2\rangle = \langle 2, \mathrm{disc}(f)\rangle$ un élément qui annule $\langle 2, \mathrm{di}(f)\rangle$ annule a fortiori $\langle 2, \mathrm{disc}(f)\rangle$. Il suffit donc de démontrer la deuxième affirmation.

Voyons le cas où $n = 2$. Un élément $z = c + dx_1 \in \mathbf{B}$ $(c, d \in \mathbf{A})$ est invariant par S_2 si et seulement si $d(x_1 - x_2) = d(a_1 - 2x_1) = 0$ si et seulement si $da_1 = 2d = 0$.

On procède ensuite par récurrence sur n. On écrit $\mathbf{B} = \mathbf{A} \oplus E$ où E est le $\mathbf{A}$-module engendré par les éléments $\neq 1$ de la base $\mathcal{B}(f)$. On note E' le sous module de E formé par les éléments fixes sous S_n. Pour $n > 2$ on considère l'anneau $\mathbf{A}_1 = \mathbf{A}[X_1]/\langle f(X_1)\rangle = \mathbf{A}[x_1]$, le polynome $F(T) = f_2(T, x_1) \in \mathbf{A}_1(T)$ et l'algèbre de décomposition universelle $\mathbf{B}_1 = \mathrm{Adu}_{\mathbf{A}_1,F}$, dans laquelle nous notons $x_2, \ldots, x_n$ les variables ($X_2, \ldots, X_n$ avant de passer au quotient). On vérifie que $\mathbf{B} \simeq \mathbf{B}_1$: une simple constatation si on utilise la définition des algèbres de décomposition universelle via les modules de Cauchy. On identifie $\mathbf{B}$ et $\mathbf{B}_1$ et on écrit $\mathbf{B}_1 = \mathbf{A}_1 \oplus E'_1$ correspondant à la base $\mathcal{B}(F)$ formée par les monomes $x_2^{d_2} \cdots x_{n-1}^{d_{n-1}}$ avec $d_i < n - i$ pour chaque i. Pour passer de l'écriture d'un élément $g \in \mathbf{B}$ sur la base $\mathcal{B}(F)$ ($\mathbf{B}$ vu comme $\mathbf{A}_1$-module) à son écriture sur la base $\mathcal{B}(f)$ ($\mathbf{B}$ vu comme $\mathbf{A}$-module), il suffit d'écrire chaque coordonnée, qui est un élément de $\mathbf{A}_1$ sur la $\mathbf{A}$-base de $\mathbf{A}_1$ formée par les monomes $1, x_1, \ldots, x_1^{n-1}$.

Notons aussi que $\mathrm{di}(f) = (-1)^{n-1}F(-x_1)\mathrm{di}(F)$ par un calcul direct et passons à la récurrence proprement dite.

Nous supposons que $\mathrm{Ann}_{\mathbf{A}}(\langle 2, \mathrm{di}(f)\rangle) = 0$. On en déduit que $\mathrm{Ann}_{\mathbf{A}_1}(\langle 2, \mathrm{di}(F)\rangle) = 0$, car si $b = \beta_0 + \beta_1 x_1 + \cdots + \beta_{n-1} x_1^{n-1} \in \mathbf{A}_1$ annule $\mathrm{di}(F)$, il annule $\mathrm{di}(f) = (-1)^{n-1} F(-x_1)\mathrm{di}(F)$, donc chacun des β_i annule $\mathrm{di}(f)$. De même chacun des β_i annule 2. Donc $b = 0$.
Soit alors $y \in E'$, écrivons $y = g(x_2, \dots x_n)$ avec $g \in \mathbf{A}_1[X_2, \dots, X_{n-1}]$ et $\deg_{X_i} g \leq n - i$ pour $i = 2, \dots, n-1$. Autrement dit nous voyons y comme un élément de $\mathrm{Adu}_{\mathbf{A}_1, F}$. Puisque y est invariant par S_{n-1}, on en déduit par hypothèse de récurrence que $g \in \mathbf{A}_1$, c'est une « constante » qu'on écrit $h(x_1)$ avec $\deg(h) < n$. Il reste à voir que $g \in \mathbf{A}$. Si $h(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$ on écrit $h(x_1) = h(x_2)$. On note que $h(x_1)$ est l'écriture réduite de g sur la base canonique $\mathcal{B}(f)$. Concernant $h(x_2)$, pour obtenir l'écriture réduite, nous devons remplacer dans le terme $c_{n-1} x_2^{n-1}$, x_2^{n-1} par son écriture sur la base canonique, qui résulte de $f_2(x_1, x_2) = 0$. Cette réécriture fait apparaître le terme $-c_{n-1} x_1^{n-2} x_2$, et ceci implique (par l'égalité des écritures $h(x_1)$ et $h(x_2)$ sur la base $\mathcal{B}(f)$) que $c_{n-1} = 0$. Mais alors $h(x_2)$ est une écriture réduite et donc tous les c_i pour $i > 0$ sont nuls. □

Remarque. Le cas $\mathrm{disc}\, f$ régulier est bien connu. On le trouve avec une preuve voisine de celle ci-dessus dans la thèse de Lionel Ducos [7]. Par ailleurs Ekedahl et Laskov ont traité le cas où 2 est régulier dans [9]. Dans le cas $n = 2$ l'étude faite ci-dessus montre que dès que $\mathrm{Ann}_{\mathbf{A}}(\langle 2, \mathrm{di}\, f\rangle) \neq 0$, $\mathrm{Fix}(\mathrm{S}_2) = \mathbf{A} \oplus \mathrm{Ann}_{\mathbf{A}}(\langle 2, \mathrm{di}\, f\rangle)\, x_1$ contient strictement $\mathbf{A}$. Un calcul dans le cas $n = 3$ donne la même réciproque : on trouve un élément $v = x_1^2 x_2 + a_1 x_1^2 + (a_1^2 + a_2) x_1 + a_2 x_2 \neq 0$ (une de ses coordonnées sur $\mathcal{B}(f)$ est égale à 1) tel que $\mathrm{Fix}(\mathrm{S}_3) = \mathbf{A} \oplus \mathrm{Ann}_{\mathbf{A}}(\langle 2, \mathrm{di}\, f\rangle)\, v$. Par contre pour $n \geq 4$, la situation se complique.

Le lemme suivant comme moyen de prouver constructivement le théorème 4.6 a été suggéré par Thierry Coquand.

Lemme 4.5 *On suppose que* $\mathrm{disc}\, f$ *est un élément inversible de* $\mathbf{A}$. *Soit* $\phi : \mathbf{A} \to \mathbf{C}$ *une algèbre dans laquelle « f se factorise complètement », c'est-à-dire* $\phi(f) = \prod_{i=1}^{n} (T - u_i)$. *Pour tout* $\sigma \in \mathrm{S}_n$ *notons* $\phi_\sigma : \mathbf{B} \to \mathbf{C}$ *l'unique homomorphisme de* $\mathbf{A}$*-algèbres qui envoie chaque* x_i *sur* $u_{\sigma i}$. *Soit* $y \in \mathbf{B}$ *tel que* $\phi_\sigma(y) = 0$ *pour tout* $\sigma \in \mathrm{S}_n$, *alors les coordonnées de y sur la base naturelle* $\mathcal{B}(f)$ *décrite dans le fait 1.3 sont dans* $\mathrm{Ker}\, \phi$.

Preuve Nous donnons la preuve pour $n = 4$ et laissons le soin au lecteur de rédiger une preuve formelle par récurrence (d'ailleurs incompréhensible si on n'a pas vu d'abord fonctionner le cas du degré 4).
On commence par remarquer que les $x_i - x_j$ sont inversibles pour $i \neq j$ et par suite les $u_i - u_j$ sont inversibles pour $i \neq j$. La base naturelle est formée par 24 éléments $x_1^{m_1} x_2^{m_2} x_3^{m_3}$ avec $0 \leq m_i \leq 4 - i$. Notons $y = a(x_1, x_2) + x_3 c(x_1, x_2)$ avec a et c des polynomes formels de degré ≤ 3 en X_1 et ≤ 2 en X_2. Notons $\overline{a}$ et $\overline{c}$ les images des polynomes formels a et c dans $\mathbf{C}$ par ϕ. Notre but est de montrer que $\overline{a}$ et $\overline{c}$ sont des polynomes identiquement nuls.
En considérant pour σ d'une part l'identité et d'autre part la transposition qui échange 3 et 4, on obtient dans $\mathbf{C}$:

$$\overline{a}(u_1, u_2) + u_3 \overline{c}(u_1, u_2) = 0 = \overline{a}(u_1, u_2) + u_4 \overline{c}(u_1, u_2)$$

Puisque $u_3 - u_4$ est inversible, on en déduit $\overline{a}(u_1, u_2) = 0 = \overline{c}(u_1, u_2)$.
La preuve qu'on vient de faire fonctionne aussi si on permute arbitrairement les x_i (on change alors de base naturelle), de sorte que $\overline{a}(u_i, u_j) = 0 = \overline{c}(u_i, u_j)$ chaque fois que $i \neq j$.
On va montrer que $\overline{a}$ est identiquement nul, la même preuve s'appliquant à $\overline{c}$. On considère $\overline{a}(u_1, X_2)$: ce polynome de degré ≤ 2 admet les trois racines u_2, u_3, u_4 et puisque les $u_i - u_j$ sont inversibles la formule d'interpolation de Lagrange montre que $\overline{a}(u_1, X_2)$ est nul comme polynome en X_2. Chacun de ses trois coefficients est un polynome de degré ≤ 3 en X_1 qu'on évalue en u_1 (on obtient ainsi 12 coordonnées de y sur la base naturelle, les 12 autres correspondant au polynome c. Notons $e(X_1)$ l'un de ces trois polynomes, lu dans $\mathbf{A}[X_1]$. La preuve que nous avons faite, montrant que $\overline{e}(u_1) = 0$ fonctionne aussi si on permute arbitrairement les x_i. Donc $\overline{e}(u_i) = 0$ pour tous les i. Encore une fois nous appliquons la formule d'interpolation de Lagrange et nous voyons que $\overline{e}(X_1)$ est identiquement nul. □

Théorème 4.6 *On suppose que* $\mathrm{disc}\, f$ *est un élément inversible de* $\mathbf{A}$.

1. *Alors le nilradical de* $\mathbf{B}$ *est l'idéal engendré par le nilradical de* $\mathbf{A}$*. En particulier, si* $\mathbf{A}$ *est réduite,* $\mathbf{B}$ *est réduite.*
2. *Pour toute algèbre réduite* $\mathbf{A} \xrightarrow{\rho} \mathbf{D}$, $\mathbf{B} \otimes_{\mathbf{A}} \mathbf{D} \simeq \mathrm{Adu}_{\mathbf{D},\rho(f)}$ *est réduite.*

Preuve Il suffit de montrer le point 1. Soit $\mathfrak{N}$ le nilradical de $\mathbf{B}$. Appliquons le lemme précédent avec $\mathbf{C} = \mathbf{B}/\mathfrak{N}$ et $y \in \mathbf{B}$ qui est nilpotent. L'élément y reste nilpotent si on le transforme par un élément de S_n. Le lemme s'applique : les coordonnées de y sur la base naturelle sont toutes dans $\mathfrak{N} \cap \mathbf{A}$. □

Le lemme 4.5 admet un frère jumeau dans le théorème qui suit, nettement plus simple d'ailleurs. On trouve une version voisine dans [7] lemme II.4.1.

Théorème 4.7 (diagonalisation d'une algèbre de décomposition universelle)
On suppose que $\mathrm{disc}\, f$ *est un élément inversible de* $\mathbf{A}$*. Soit* $\phi : \mathbf{A} \to \mathbf{C}$ *une algèbre dans laquelle « f se factorise complètement », c'est-à-dire* $\phi(f) = \prod_{i=1}^{n}(T - u_i)$*. On considère* $\mathbf{C}_1 = \mathbf{B} \otimes_{\mathbf{A}} \mathbf{C} \simeq \mathrm{Adu}_{\mathbf{C},\phi(f)}$*. Pour tout* $\sigma \in \mathrm{S}_n$ *notons* $\phi_\sigma : \mathbf{C}_1 \to \mathbf{C}$ *l'unique homomorphisme de* $\mathbf{C}$*-algèbres qui envoie chaque* $x_i \otimes 1_{\mathbf{C}}$ *sur* $u_{\sigma i}$*. Soit* $\Phi : \mathbf{C}_1 \to \mathbf{C}^{n!}$ *l'homomorphisme de* $\mathbf{C}$*-algèbres défini par* $y \mapsto (\phi_\sigma(y))_{\sigma \in \mathrm{S}_n}$*.*

1. Φ *est un isomorphisme :* $\mathbf{C}$ *diagonalise* $\mathbf{B}$*.*
2. *Plus précisément notons* $g_\sigma = \prod_{i=1}^{n}\prod_{j \neq \sigma i}(x_i - u_j)$*. Alors* $\phi_\sigma(g_\sigma) = \pm\mathrm{disc}(f)^n$ *et* $\phi_\sigma(g_\tau) = 0$ *pour* $\tau \neq \sigma \in \mathrm{S}_n$*, de sorte que si on pose* $e_\sigma = g_\sigma/\phi_\sigma(g_\sigma)$*, les* e_σ *forment le sfio correspondant à l'isomorphisme* Φ*.*
3. *En outre* $u_i e_\sigma = x_{\sigma i} e_\sigma$*, de sorte que la base* (e_σ) *du* $\mathbf{C}$*-module* $\mathbf{C}_1$ *est une base diagonale commune pour les multiplications par les* x_i*.*

En particulier $\mathbf{B} \otimes_{\mathbf{A}} \mathbf{B} \simeq \mathrm{Adu}_{\mathbf{B},f}$ *est isomorphe canoniquement à* $\mathbf{B}^{n!}$ *:* $\mathbf{B}$ *se diagonalise elle-même. NB : Il faut prendre garde cependant à noter* $\mathrm{Adu}_{\mathbf{B},f} = \mathbf{B}[u_1, \ldots, u_n]$ *puisque les* x_i *sont déjà pris comme éléments de* $\mathbf{B}$*.*

Preuve Voyons le point 1). Les deux algèbres sont en tant que $\mathbf{C}$-modules isomorphes à $\mathbf{C}^{n!}$ et Φ est une application $\mathbf{C}$-linéaire dont il suffit de démontrer la surjectivité. Dans $\mathbf{C}_1$ nous notons x_i à la place de $x_i \otimes 1_{\mathbf{C}}$, et u_i à la place de $1_{\mathbf{B}} \otimes u_i$ (conformément à la structure de $\mathbf{C}$-algèbrede $\mathbf{C}_1$). La surjectivité résulte par le théorème chinois de ce que les $\mathrm{Ker}\,\phi_\sigma$ sont deux à deux comaximaux : $\mathrm{Ker}\,\phi_\sigma$ contient $x_i - u_{\sigma i}$, $\mathrm{Ker}\,\phi_\tau$ contient $x_i - u_{\tau i}$, donc $\mathrm{Ker}\,\phi_\sigma + \mathrm{Ker}\,\phi_\tau$ contient les $u_{\sigma i} - u_{\tau i}$, et il y a au moins un indice i pour lequel $\sigma i \neq \tau i$ ce qui donne $u_{\sigma i} - u_{\tau i}$ inversible.
Pour les points 2 et 3, on note que le sfio correspondant à l'isomorphisme Φ est l'unique solution du système d'équations $\phi_\sigma(e_\tau) = \delta_{\sigma,\tau}$ où δ est le symbole de Kronecker. Et les égalités $\phi_\sigma(g_\sigma) = \pm\mathrm{disc}(f)^n$, $\phi_\sigma(g_\tau) = 0$ et $u_i g_\sigma = x_{\sigma i} g_\sigma$ sont faciles. □

Remarque. En fait Φ est une application linéaire dont on devrait pouvoir calculer le déterminant par rapport aux bases naturelles, éventuellement en utilisant un cas générique simple. Ce déterminant doit simplement être le discriminant ou une puissance du discriminant. On obtiendrait donc que $\mathbf{C}$ diagonalise $\mathbf{B}$ si et seulement si $\mathrm{disc}\, f$ est inversible dans $\mathbf{C}$.

Le théorème précédent peut être résumé sous la forme : toute $\mathbf{B}$-algèbre diagonalise $\mathbf{B}$. Nous en donnons maintenant une généralisation pour un quotient de Galois de $\mathbf{B}$.

Théorème 4.8 (diagonalisation d'un quotient de Galois d'une algèbre de décomposition universelle)
On suppose que $\mathrm{disc}\, f$ *est un élément inversible de* $\mathbf{A}$*. Soit* e *un idempotent galoisien de* $\mathbf{B}$ *et* $\mathbf{B}_1 = \mathbf{B}/\langle 1 - e \rangle$*. On note* $y_i = \pi(x_i)$ *la classe de* x_i *dans* $\mathbf{B}_1$*. Soit* $\phi : \mathbf{B}_1 \to \mathbf{C}$ *un homomorphisme d'anneaux. On note* $u_i = \phi(y_i)$*. On considère* $\mathbf{C}_1 = \mathbf{B}_1 \otimes_{\mathbf{A}} \mathbf{C}$*. Pour tout* $\sigma \in \mathrm{S}_n$ *notons* $\phi_\sigma : \mathbf{C}_1 \to \mathbf{C}$ *l'unique homomorphisme de* $\mathbf{C}$*-algèbres qui envoie chaque* $y_i \otimes 1_{\mathbf{C}}$ *sur* $u_{\sigma i}$*. Soit* $\Phi : \mathbf{C}_1 \to \mathbf{C}^{|G|}$ *l'homomorphisme de* $\mathbf{C}$*-algèbres défini par* $z \mapsto (\phi_\sigma(z))_{\sigma \in G}$*.*

1. Φ *est un isomorphisme :* $\mathbf{C}$ *diagonalise* $\mathbf{B}_1$*.*
2. *En particulier* $\mathbf{B}_1 \otimes_{\mathbf{A}} \mathbf{B}_1$ *est isomorphe canoniquement à* $\mathbf{B}_1^{|G|}$ *:* $\mathbf{B}_1$ *se diagonalise elle-même.*

Preuve Les deux algèbres sont des $\mathbf{C}$-modules projectifs de rang constant $|G|$ et Φ est une application $\mathbf{C}$-linéaire dont il suffit de démontrer la surjectivité. Dans $\mathbf{C}_1$ nous notons y_i à la place de $y_i \otimes 1_{\mathbf{C}}$ et u_i à la place de $1_{\mathbf{B}_1} \otimes u_i$. La surjectivité résulte par le théorème chinois de ce que les $\operatorname{Ker}\phi_\sigma$ sont deux à deux comaximaux : $\operatorname{Ker}\phi_\sigma$ contient $y_i - u_{\sigma i}$, $\operatorname{Ker}\phi_\tau$ contient $y_i - u_{\tau i}$, donc $\operatorname{Ker}\phi_\sigma + \operatorname{Ker}\phi_\tau$ contient les $u_{\sigma i} - u_{\tau i}$, et il y a au moins un indice i pour lequel $\sigma i \neq \tau i$ ce qui donne $u_{\sigma i} - u_{\tau i}$ inversible. □

5 Structure triangulaire des idéaux galoisiens

Nous démontrons dans cette section le théorème 5.2 qui généralise un résultat donné séparément dans le cas de l'algèbre de décomposition universelle sur un corps par L. Ducos [8] et par P. Aubry et A. Valibouze [1]. Ce résultat affirme que la structure de l'idéal $\mathcal{J}(f)$, qui est une structure « triangulaire » (au sens de Lazard) lorsqu'on considère les modules de Cauchy comme générateurs, se retrouve pour tous les idéaux galoisiens de l'algèbre de décomposition universelle dans le cas d'un polynome séparable sur un corps.

Notre méthode de preuve se rapproche plus de celle de L. Ducos, mais elle est différente car le cadre est nettement plus plus général : nous avons à la base un anneau commutatif presque arbitraire à la place d'un corps et l'algèbre est une algèbre galoisienne générale.

Définition 5.1 (idéaux galoisiens) *Soit* $(\mathbf{A}, \mathbf{C}, G)$ *une algèbre prégaloisienne. Un idéal de* $\mathbf{C}$ *est dit* galoisien *lorsqu'il est engendré par l'idempotent complémentaire d'un idempotent galoisien.*

Les anneaux que nous considérons sont les anneaux $\mathbf{A}$ qui vérifient la propriété suivante : l'anneau total des fractions de $\mathbf{A}$, $\operatorname{Frac}\mathbf{A}$, est zéro-dimensionnel. C'est notamment le cas des anneaux intègres, des anneaux zéro-dimensionnels et des anneaux nœthériens.

Nous aurons besoin des résultats suivants que nous utilisons librement dans la preuve du théorème.
- Si $(\mathbf{A}, \mathbf{C}, G)$ une algèbre galoisienne, $\mathbf{C}$ est un $\mathbf{A}$-module projectif de rang $|G|$, et $\mathbf{A}$ est facteur direct dans $\mathbf{C}$.
- Si $\mathbf{A}$ est zéro-dimensionnel, tout module projectif de rang constant est libre.
- Si $\mathbf{A}$ est zéro-dimensionnel, et si $N \subset \mathbf{A}^n$ est libre, il existe $M \subset \mathbf{A}^n$ libre tel que $\mathbf{A}^n = M \oplus N$ (théorème de la base incomplète).

Le théorème 5.2 s'applique pour l'algèbre de décomposition universelle dans la situation suivante : On suppose le polynome f séparable. On considère un idempotent galoisien $e = 1 - s$ et l'idéal galoisien correspondant $\mathfrak{b} = \langle s \rangle$. On pose

$$\mathbf{C} = \mathbf{B}/\mathfrak{b} = \mathbf{A}[X_1, \ldots, X_n]/\mathfrak{a} = \mathbf{A}[y_1, \ldots, y_n]$$

avec :
- y_i est la classe de x_i modulo $\mathfrak{b}$ ou de X_i modulo $\mathfrak{a}$,
- $\mathfrak{a} = \mathcal{J}(f) + \langle S \rangle$ si $S \in \mathbf{A}[X_1, \ldots, X_n]$ et $s = S(x_1, \ldots, x_n)$.

On note $G = G_0 = \operatorname{St}(e) = \operatorname{St}(\mathfrak{b}) \subset \mathrm{S}_n$, on le considère comme un groupe de $\mathbf{A}$-automorphismes de $\mathbf{C}$.

On sait alors que $(\mathbf{A}, \mathbf{C}, G)$ est une algèbre galoisienne. En effet $\mathbf{A} = \operatorname{Fix}(G)$ et un élément σ de G distinct de l'identité ne fixe pas tous les y_i et donc l'un des $y_i - \sigma(y_i)$ engendre l'idéal $\langle 1 \rangle$ de $\mathbf{C}$ car les $y_i - y_j$ sont inversibles pour $i \neq j$.

Théorème 5.2 *Soit* $(\mathbf{A}, \mathbf{C}, G)$ *une algèbre galoisienne avec*
- $\mathbf{C} = \mathbf{A}[y_1, \ldots, y_n]$,
- G *opère sur* $\{y_1, \ldots, y_n\}$ *et*
- *les* $y_i - y_j$ *inversibles pour* $i \neq j$.

On suppose que l'anneau total des fractions de $\mathbf{A}$, $\operatorname{Frac}\mathbf{A}$, *est zéro-dimensionnel. On note* $G = G_0$, $G_i = \{\sigma \in G\,;\, \sigma(y_k) = y_k,\ \forall k \leq i\}$, *(*$i = 1 \ldots, n$*), et*

$$r_i(T) = \prod_{\sigma \in G_{i-1}/G_i} (T - \sigma(y_i))$$

où G_{i-1}/G_i *désigne un système de représentants des classes à gauche. Alors :*

- $\mathbf{A}[y_1,\dots,y_i] = \mathrm{Fix}(G_i)$ *et* $G_i = \mathrm{Stp}(\mathbf{A}[y_1,\dots,y_i])$.
- $r_i(T)$ *est un polynome unitaire de degré* $(G_{i-1} : G_i)$ *à coefficients dans* $\mathbf{A}[(y_k)_{k<i}]$, *on note* $R_i(X_1,\dots,X_i)$ *un polynome unitaire de degré* $(G_{i-1} : G_i)$ *de* $\mathbf{A}[X_1,\dots,X_i]$ *tel que* $R_i(y_1,\dots,y_{i-1},X_i) = r_i(X_i)$.
- *L'idéal* $\mathfrak{a}_i = \mathfrak{a} \cap \mathbf{A}[X_1,\dots,X_i]$ *est engendré par* $R_1(X_1),\dots,R_i(X_1,\dots,X_i)$.

En conséquence chacune des algèbres $\mathbf{A}[y_1,\dots,y_i]$ *est à la fois un* $\mathbf{A}[y_1,\dots,y_{i-1}]$*-module libre de rang* $(G_{i-1} : G_i)$ *et un* $\mathbf{A}$*-module libre de rang* $(G : G_i)$, *et chacun des idéaux* $\mathfrak{a}_i$ *est un idéal triangulaire (au sens de Lazard) de* $\mathbf{A}[X_1,\dots,X_i]$.

Preuve Le groupe G_1 est un groupe séparant d'automorphismes de l'anneau $\mathbf{C}$. On note $\mathbf{A}_1$ l'anneau des points fixes de G_1. On sait que $\mathbf{C}$ est un $\mathbf{A}_1$-module projectif de rang constant $|G_1|$ et que $\mathbf{A}[y_1] \subset \mathbf{A}_1$. En outre $\mathbf{A}_1$ est facteur direct dans $\mathbf{C}$, donc est un $\mathbf{A}$-module projectif de rang constant $|G|/|G_1|$. Les coefficients de $r_1(T)$ sont fixes par G, donc dans $\mathbf{A}$, parce que les $\sigma(y_1)$ pour $\sigma \in G/G_1$ parcourent l'orbite de y_1 sous G. En outre $\deg r_1 = (G : G_1)$, de sorte que $\mathbf{A}[X_1]/\langle r_1(X_1)\rangle$ est libre de rang $(G : G_1)$. L'idéal $\mathfrak{a}_1$ est formé par tous les $R \in \mathbf{A}[X_1]$ qui annulent y_1. Un tel polynome R vérifie $R(\sigma(y_1)) = 0$ pour tout $\sigma \in G/G_1$ parce que ses coefficients sont dans $\mathbf{A}$ et que σ fixe tous les éléments de $\mathbf{A}$. Donc R est multiple des $(T-\sigma(y_1))$. Or les idéaux $\langle T - y_i\rangle$ sont deux à deux comaximaux (parce que les $y_i - y_j$ sont inversibles), et l'intersection d'idéaux deux à deux comaximaux est égale à leur produit, donc R est multiple de r_1. Ainsi $\mathfrak{a}_1 = \langle r_1(X_1)\rangle$ et $\mathbf{A}[y_1]$ est libre de rang $(G : G_1)$.
On a donc la situation suivante :

- $\mathbf{A}_1$ est un $\mathbf{A}$-module projectif de rang constant $|G|/|G_1|$,
- $\mathbf{A}[y_1]$ est libre de rang $|G|/|G_1|$,
- $\mathbf{A}[y_1] \subset \mathbf{A}_1$.

Supposons maintenant l'anneau $\mathbf{A}$ zéro-dimensionnel. Alors $\mathbf{A}_1$ est libre sur $\mathbf{A}$, et $\mathbf{A}[y_1] = \mathbf{A}_1$ par le théorème de la base incomplète. Donc $\mathbf{A}[y_1] = \mathbf{A}_1 = \mathrm{Fix}(G_1)$ et $(\mathbf{A}[y_1], \mathbf{C}, G_1)$ est une algèbre galoisienne. Alors $\mathbf{C} = \mathbf{A}_1[y_2,\dots,y_n]$ avec G_1 qui opère sur $\{y_2,\dots,y_n\}$ et les $y_i - y_j$ inversibles. Tout le raisonnement précédent fonctionne à l'identique en remplaçant $\mathbf{A}$ par $\mathbf{A}_1$, G par G_1, y_1 par y_2 et G_1 par G_2. On termine donc par récurrence.

Passons au cas général. Nous avons de nouveau $\mathbf{A}[y_1] \simeq \mathbf{A}[X_1]/\langle r_1(X_1)\rangle$ et $\mathbf{A}[y_1] \subset \mathbf{A}_1 = \mathrm{Fix}(G_1)$. Notons S l'ensemble des éléments réguliers de $\mathbf{A}$ et $\mathbf{F} = \mathrm{Frac}\,\mathbf{A} = S^{-1}\mathbf{A}$. Remarquons que puisqu'un élément régulier de $\mathbf{A}$ est régulier dans $\mathbf{C}$ on a $\mathbf{C} \subset S^{-1}\mathbf{C} = \mathbf{C} \otimes_{\mathbf{A}} \mathbf{F}$. Le cas zéro-dimensionnel implique que $S^{-1}\mathbf{A}_1 = S^{-1}\mathbf{A}[y_1]$, et notre objectif est de montrer l'égalité $\mathbf{A}_1 = \mathbf{A}[y_1]$. Soit donc $z \in \mathbf{A}_1$ et $s \in S$ tel que $sz \in \mathbf{A}[y_1]$: $sz = c_0 + c_1y_1 + \cdots + c_{d_1-1}y_1^{d_1-1}$. Posons $s_k = \sum_{\sigma\in G/G_1} \sigma(y_1)^k$. Ce sont les sommes de Newton pour le polynome $r_1 = R_1$, donc des éléments de $\mathbf{A}$. On a

$$szy_1^k = c_0y_1^k + c_1y_1^{k+1} + \cdots + c_{d_1-1}y_1^{k+d_1-1}.$$

donc pour un $\sigma \in G/G_1$, si $\sigma(y_1) = y_\ell$:

$$s\sigma(zy_1^k) = c_0y_\ell^k + c_1y_\ell^{k+1} + \cdots + c_{d_1-1}y_\ell^{k+d_1-1}.$$

Comme $zy_1^k \in \mathbf{A}_1$ on a $\sum_{\sigma\in G/G_1} \sigma(zy_1^k)$ fixe par G donc dans $\mathbf{A}$ et $s\sum_{\sigma\in G/G_1} \sigma(zy_1)^k = c_0s_k + \cdots + c_{d_1-1}s_{k+d_1-1} \in s\mathbf{A}$. Sous forme matricielle :

$$\begin{bmatrix} s_0 & s_1 & s_2 & \cdots & s_{d_1-1} \\ s_1 & s_2 & & \cdots & s_{d_1} \\ \vdots & & & & \vdots \\ s_{d_1-1} & \cdots & \cdots & \cdots & s_{2d_1-2} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{d_1-1} \end{bmatrix} \in s\mathbf{A}^{d_1\times 1}$$

or le déterminant de la matrice carrée au premier membre est égal au discriminant de r_1 donc est inversible. Ainsi les c_j sont tous multiples de s. □

6 Corps des racines

Dans cette section, qui aurait pu être placée en position 4, nous remplaçons l'anneau **A** par un corps discret **K** et nous expliquons comment l'algèbre de décomposition universelle permet d'obtenir le corps des racines d'un polynome, ou au moins un substitut constructif de ce dernier.

Dans la section 6 **K** est un corps discret, f est un polynome unitaire de degré n et $\mathbf{B} = \mathrm{Adu}_{\mathbf{K},f}$.

Une **K**-algèbre est dite *finie* si c'est un **K**-espace vectoriel de type fini (en mathématiques constructives cela n'implique pas qu'on connaisse une base de l'espace vectoriel), *strictement finie* si c'est un **K**-espace vectoriel de dimension finie.

Les quotients de l'algèbre de décomposition universelle $\mathbf{B} = \mathrm{Adu}_{\mathbf{K},f}$ sont des **K**-algèbres finies et toute **K**-algèbre finie est un annneau *zéro-dimensionnel*.

Nous commençons par le rappel de quelques faits de base concernant ces anneaux.

Anneaux zéro-dimensionnels

Fait 6.1 *Dans un anneau* **C**, *si* $x^k(1-ax)=0$, *l'élément* $e = x^k a^k$ *est idempotent,* $\langle x^k\rangle = \langle e\rangle$, *et* x *est inversible dans* $\mathbf{C}[1/e]$ *et nilpotent dans* $\mathbf{C}[1/(1-e)]$.

Définition 6.2 *Un anneau* **C** *est zéro-dimensionnel si pour tout* x *il existe un* $a \in \mathbf{C}$ *et un* $k \in \mathbb{N}$ *tel que* $x^k(1-ax)=0$.

Fait 6.3

1. *Si* x *est un élément d'un anneau zéro-dimensionnel il existe un unique idempotent* e_x *tel que* x *est inversible dans* $\mathbf{C}[1/e_x]$ *et nilpotent dans* $\mathbf{C}[1/(1-e_x)]$. *En particulier,* x *est inversible si et seulement si* $e_x = 1$, *nilpotent si et seulement si* $e_x = 0$.
2. *Un quotient ou un localisé d'un anneau zéro-dimensionnel est zéro-dimensionnel. Un produit fini d'anneaux zéro-dimensionnels est zéro-dimensionnel.*
3. *Dans un anneau zéro-dimensionnel le radical de Jacobson est égal au nilradical, tout élément régulier est inversible.*
4. *Un anneau zéro-dimensionnel connexe est local.*
5. *Un anneau est local et zéro-dimensionnel si et seulement si tout élément est inversible ou nilpotent.*
6. *Un anneau zéro-dimensionnel réduit connexe est un corps discret.*
7. *Si* **K** *est un corps discret toute* **K***-algèbre entière* **C**, *donc en particulier une algèbre de décomposition universelle sur* **K**, *est un anneau zéro-dimensionnel.*

Preuve Nous rappelons juste l'algorithme pour le point 7. Soit $x \in \mathbf{C}$ et $h(T)$ un polynome unitaire qui annule x. Si $h(0) \neq 0$, x est inversible. Sinon, soit h_k le coefficient non nul de plus bas degré, on écrit $h(T) = h_k T^k(1 - Tg(T))$, de sorte que $x^k(1-ax)=0$ avec $a = g(x)$. □

Fait 6.4 *Soit* **C** *un anneau zéro-dimensionnel.*

1. *On a* $\mathbb{B}(\mathbf{C}) \simeq \mathbb{B}(\mathbf{C}/\sqrt{0})$ *: tout idempotent de* $\mathbf{C}/\sqrt{0}$ *se relève en un unique idempotent de* **C**.
2. *Si* $\mathfrak{a}$ *est un idéal de type fini alors il existe un entier* ℓ *et un idempotent* e *tels que* $\mathfrak{a}^\ell = \langle e\rangle$. *Alors* $\mathfrak{a}^{\ell+r} = \mathfrak{a}^\ell$ *pour tout* $r \geq 0$, *l'idéal* $\mathfrak{a}$ *devient égal à* $\langle 1\rangle$ *dans* $\mathbf{C}[1/e]$ *et nilpotent dans* $\mathbf{C}[1/(1-e)]$, *et* $\sqrt{\mathfrak{a}} = \sqrt{\langle e\rangle}$. *En particulier* $\mathrm{Zar}\,\mathbf{C} \simeq \mathbb{B}(\mathbf{C})$.
3. *Pour un idempotent* e *les propriétés suivantes sont équivalentes :*
   (a) e *est indécomposable.*
   (b) $\mathbf{C}/\langle 1-e\rangle$ *est un anneau local.*

(c) $\mathbf{C}\Big/\sqrt{\langle 1-e\rangle}$ *est un anneau local.*

(d) $\mathbf{C}\Big/\sqrt{\langle 1-e\rangle}$ *est un corps discret.*

4. *Les propriétés suivantes sont équivalentes :*

(a) $\mathbb{B}(\mathbf{C})$ *est finie.*

(b) $\mathbf{C}$ *est isomorphe à un produit fini d'anneaux locaux zéro-dimensionnels.*

(c) $\mathbf{C}/\sqrt{0}$ *est isomorphe à un produit fini de corps discrets.*

Quotients réduits de l'algèbre de décomposition universelle

Lemme 6.5 *Soit $\mathbf{C}$ une $\mathbf{K}$-algèbre strictement finie telle que f se décompose totalement dans $\mathbf{C}/\sqrt{0}$. On suppose en outre que $\mathbf{C}/\sqrt{0}$ est engendrée par les zéros correspondants de f. Alors il existe un idempotent e de $\mathbf{B} = \mathrm{Adu}_{\mathbf{K},f}$ tel que $\mathbf{C}/\sqrt{0} \simeq \mathbf{B}\Big/\sqrt{\langle 1-e\rangle}$.*

Preuve Soit $y_1, \ldots, y_n \in \mathbf{C}$ tels que $f(T) = \prod_i (T - \overline{y_i})$ dans $\mathbf{C}/\sqrt{0}$. Par ailleurs $\mathbf{B} = \mathbf{K}[X_1, \ldots, X_n]/\mathcal{J}(f)$ et on a un unique homomorphisme $\lambda : \mathbf{K}[X_1, \ldots, X_n] \to \mathbf{C}$ qui envoie les X_i sur les y_i. On a alors $\lambda(\mathcal{J}(f)) \subseteq \sqrt{0}$. Puisque $\lambda(\mathcal{J}(f))$ est un idéal de type fini, $\mathbf{C}_1 := \mathbf{C}/\lambda(\mathcal{J}(f))$ est une $\mathbf{K}$-algèbre strictement finie. On a alors $\mathbf{C}/\sqrt{0} \simeq \mathbf{C}_1/\sqrt{0}$ et on a un unique homomorphisme $\varphi : \mathbf{B} \to \mathbf{C}_1$ qui envoie x_i sur la classe de y_i. Dans $\mathbf{C}_1$, $(\sqrt{0})^k = \langle 0\rangle$ si k est la dimension de $\mathbf{C}_1$ comme $\mathbf{K}$-espace vectoriel. Finalement on obtient $1 - e$ comme générateur de l'idéal $(\operatorname{Ker}\varphi)^k$. □

En mathématiques classiques un corps des racines pour un polynome unitaire f sur un corps discret $\mathbf{K}$ est obtenu en quotientant l'algèbre de décomposition universelle $\mathrm{Adu}_{\mathbf{K},f}$ par un idéal $\sqrt{\langle 1-e\rangle}$ où e est un idempotent indécomposable (qui existe d'après le théorème 3.4, ou bien simplement en considérant un idéal non nul dont la dimension comme $\mathbf{K}$-espace vectoriel est minimale).

En mathématiques constructives on obtient le théorème plus précis qui suit.

Théorème 6.6 *Les propriétés suivantes sont équivalentes :*

1. *Il existe dans $\mathbf{B} = \mathrm{Adu}_{\mathbf{K},f}$ un idempotent indécomposable e.*
2. *Il existe une extension $\mathbf{L}$ de $\mathbf{K}$ qui est un corps des racines de f et qui s'écrit $\mathbf{C}/\sqrt{0}$ où $\mathbf{C}$ est une $\mathbf{K}$-algèbre strictement finie.*
3. *L'algèbre de Boole $\mathbb{B}(\mathbf{B})$ est finie.*

Dans ce cas tout corps des racines de f est isomorphe à $\mathbf{B}\Big/\sqrt{\langle 1-e\rangle}$. Il est discret.
En particulier, si pour le polynome f un corps des racines existe et est de dimension finie, deux corps des racines pour f sont isomorphes.

Preuve L'équivalence de 1 et 3 vaut dans le cadre général des algèbres de Boole (théorème 3.4).
Il est clair que 1 implique 2. Inversement si on a un corps des racines $\mathbf{L} = \mathbf{C}/\sqrt{0}$ où $\mathbf{C}$ est une $\mathbf{K}$-algèbre strictement finie, on calcule l'idempotent correspondant e en appliquant le lemme 6.5, et celui-ci est indécomposable d'après le fait 6.4.
Voyons l'unicité. Soit $\mathbf{M}$ un corps des racines pour f. Notez que nous ne supposons pas $\mathbf{M}$ discret. Écrivons $f(T) = \prod_{i=1}^{n}(T - \xi_i)$ dans $\mathbf{M}$. Par la propriété universelle des algèbres de décomposition universelle (fait 1.1) il existe un unique homomorphisme de $\mathbf{K}$-algèbres $\varphi : \mathbf{B} \to \mathbf{M}$ tel que $\varphi(x_i) = \xi_i$ pour $i = 1, \ldots, n$. Soit $(e_j)_{j=1,\ldots,k}$ l'orbite de e. Chaque $\varphi(e_j)$ est un idempotent et leur somme est égale à 1, puisque $\mathbf{M}$ est un anneau local cela implique qu'il y a un j pour lequel $\varphi(e_j) = 1$. Alors $\mathbf{M}$ est un quotient de $\mathbf{B}_j = \mathbf{B}\Big/\sqrt{\langle 1-e_j\rangle}$, qui est un corps discret. Comme $\mathbf{M}$ est supposé non trivial, cela implique $\operatorname{Ker}\varphi = \sqrt{\langle 1-e_j\rangle}$ et $\mathbf{M} \simeq \mathbf{B}_j$. Et les B_j sont deux à deux isomorphes. □

Commentaire. Dans [10], il est montré que tout corps discret énumérable possède une cloture algébrique. Cependant, un corps des racines pour f, qui existe donc, ne possède pas nécessairement une base finie comme $\mathbf{K}$-espace vectoriel, au sens des mathématiques constructives. Et on ne connaît

pas de théorème d'unicité constructif pour un tel corps de racines. On peut mimer comme suit ce que ferait Richman pour obtenir un corps des racines pour f : on énumère l'algèbre de décomposition universelle $(z_m)_{m\in\mathbb{N}}$, on construit un idéal de type fini $\mathfrak{a}_m$ de $\mathbf{B}$ en posant $\mathfrak{a}_0 = 0$ et $\mathfrak{a}_{m+1} = \mathfrak{a}_m + \langle z_m\rangle$ si $\mathfrak{a}_m + \langle z_m\rangle \neq \langle 1\rangle$ et $\mathfrak{a}_{m+1} = \mathfrak{a}_m$ sinon. Alors l'idéal $\bigcup_m \mathfrak{a}_m$ est un idéal maximal de $\mathbf{B}$ et le quotient est un corps des racines, qui est discret. Notre point de vue est légèrement différent. Nous ne partons pas a priori d'un corps énumérable, et même dans le cas d'un corps énumérable, nous ne privilégions pas une énumération par rapport à une autre. Nous nous contentons plutôt de répondre aux questions concernant le corps des racines au fur et à mesure qu'elles se posent.

Le théorème suivant explique comment contourner la difficulté que pose la non existence du corps des racines en mathématiques constructives.

Théorème 6.7 *Soit $(z_i)_{i\in I}$ une famille finie d'éléments de $\mathbf{B} = \mathrm{Adu}_{\mathbf{K},f}$. Il existe un idempotent galoisien e_1 de $\mathbf{B}$ tel que chaque $\pi(z_i)$ est nul ou inversible dans l'algèbre quotient $\mathbf{B}_1 = \mathbf{B}\Big/\sqrt{\langle 1-e_1\rangle}$ (π est la projection canonique $\mathbf{B}\to\mathbf{B}_1$).*

Preuve Pour chaque $i\in I$ on calcule un idempotent $g_i\in\mathbf{B}$ (fait 6.3 (7) et fait 6.1) : z_i est inversible modulo $1-g_i$ et nilpotent modulo g_i. Appliqué à la famille des g_i le théorème 3.4 donne un idempotent galoisien e_1, tel que pour chaque i, $1-e_1$ divise g_i ou $1-g_i$. Donc dans l'algèbre quotient $\mathbf{B}_1 = \mathbf{B}/\langle 1-e_1\rangle$ chaque $\pi(z_i)$ est nilpotent ou inversible. □

Remarque. Naturellement, dans le théorème précédent on a intérêt à saturer la famille $(z_i)_{i\in I}$ par l'action de S_n de façon à rendre manifestes dans $\mathbf{B}_1$ tous les « cas de figure » possibles.

Le théorème d'unicité du corps des racines admet une version constructive « opératoire » (qui fonctionne à tout coup, même si on ne dispose pas d'un idempotent indécomposable dans l'algèbre de décomposition universelle) sous la forme suivante :

Théorème 6.8 *Soient deux $\mathbf{K}$-algèbres strictement finies $\mathbf{A}_1$ et $\mathbf{A}_2$ non nulles pour lesquelles f se décompose en produit de facteurs linéaires dans $\mathbf{C}_1 = \mathbf{A}_1/\sqrt{0}$ et $\mathbf{C}_2 = \mathbf{A}_2/\sqrt{0}$. On suppose en outre que $\mathbf{C}_1$ et $\mathbf{C}_2$ sont engendrées par les zéros correspondants de f. Alors il existe une $\mathbf{K}$-algèbre $\mathbf{C} = \mathbf{B}\Big/\sqrt{\langle 1-e\rangle}$ (e idempotent galoisien) avec les mêmes propriétés, et deux entiers r_i tels que $\mathbf{C}_1\simeq\mathbf{C}^{r_1}$ et $\mathbf{C}_2\simeq\mathbf{C}^{r_2}$.*

Preuve Le lemme 6.5 nous fournit deux idempotents correspondant aux quotients $\mathbf{C}_1$ et $\mathbf{C}_2$ de $\mathbf{B}$ et le théorème 3.4 nous donne un idempotent galoisien qui les raffine tous les deux. □

Cas d'un polynome séparable

On suppose maintenant que f est séparable. l'algèbre de décomposition universelle est alors réduite d'après le théorème 4.6. La situation est alors un peu plus simple, conformément au lemme suivant.

Lemme 6.9 *Soit $\mathbf{C}$ un anneau zéro-dimensionnel réduit, par exemple une $\mathbf{K}$-algèbre finie réduite.*

1. *Tout idéal de type fini de $\mathbf{C}$ est engendré par un idempotent.*
2. *Tout idéal $\mathfrak{c}$ de $\mathbf{C}$ est égal à son radical $\sqrt{\mathfrak{c}}$.*

Nous laissons le soin au lecteur de réécrire les résultats précédents en tenant compte du lemme 6.9 et nous terminons par la preuve constructive d'un résultat classique.

Contrairement à ce qui se passe dans les preuves classiques usuelles, le résultat fondamental suivant est obtenu sans utiliser le corps des racines (seule une approximation convenable suffit).

Théorème 6.10 *Soit $\mathbf{K}$ un corps discret et $f\in\mathbf{K}[X]$ un polynome séparable.*

1. *L'algèbre de décomposition universelle $\mathbf{B} = \mathrm{Adu}_{\mathbf{K},f}$ est séparable (i.e., tout élément annule un polynome séparable de $\mathbf{K}[T]$).*

2. *Si e est un idempotent l'algèbre quotient $\mathbf{B}/\langle 1-e\rangle$ est séparable.*

Preuve Si $\mathbf{K}$ est de caractéristique nulle, un polynome est séparable si et seulement si il est sans facteur carré. Le fait que $\mathbf{B}$ est réduite implique alors que le polynome minimal de tout élément de $\mathbf{B}$ est séparable.
Dans le cas général, la preuve est un peu plus compliquée. Soit $z \in \mathbf{B}$. Appliqué à la famille des $\sigma(z)-\tau(z)$ ($\sigma \neq \tau$ dans S_n) le théorème 6.7 donne un idempotent galoisien e_1 tel que dans l'algèbre quotient $\mathbf{B}_1 = \mathbf{B}/\langle 1-e_1\rangle$ chaque $\pi_1(\sigma(z)-\tau(z))$ est nul ou inversible (π_1 est la projection canonique $\mathbf{B} \to \mathbf{B}_1$). On rappelle que d'après les théorèmes 2.3 et 4.4, le stabilisateur G de e_1 opère sur $\mathbf{B}_1$ et les points fixes pour cette action sont exactement les éléments de $\mathbf{K}$ (identifié à $\pi_1(\mathbf{K})$). Soit alors $\{z_1,\dots,z_t\}$ un ensemble de S_n-conjugués de z tels que $\{\pi_1(z_1),\dots,\pi_1(z_t)\}$ soit l'orbite de $\pi_1(z)$ pour l'action de G. On considère le polynome $P_1(T) = \prod_{i=1}^{t}(T-\pi_1(z_i))$. Ses coefficients sont fixés par G donc $P_1 \in \mathbf{K}[T]$. Et c'est un polynome séparable par construction (comme polynome dans $\mathbf{B}_1[T]$ son discriminant est inversible). Ainsi $\pi_1(z)$ annule le polynome séparable $P_1(T) \in \mathbf{K}[T]$, c'est-à-dire encore $P_1(z) \in \langle 1-e_1\rangle$. Si $\{e_1,\dots,e_k\}$ est l'orbite de e_1 sous S_n, on aura pour $i=1,\dots,k$ un polynome séparable $P_i \in \mathbf{K}[T]$ avec $P_i(z) \in \langle 1-e_i\rangle$. Finalement le ppcm P des P_i est lui-même un polynome séparable de $\mathbf{K}[T]$ et $P(z) \in \bigcap_i \langle 1-e_i\rangle = \langle 0\rangle$.
Enfin le point 2 résulte du premier : si $z \in \mathbf{B}$, et y est son image dans $\mathbf{B}/\langle 1-e\rangle$, un polynome séparable qui annule z annule y. □

Références

[1] Aubry P., Valibouze A. *Using Galois Ideals for Computing Relative Resolvents.* J. Symbolic Computation, **30**, (2000), 635–651. 13

[2] Bishop E., Bridges D. *Constructive Analysis.* Springer-Verlag (1985). 2, 7

[3] Bourbaki *Algèbre. Chap 4 à 7.* Masson. Paris (1981). 2

[4] Della Dora J., Dicrescenzo C., Duval D. *About a new method for computing in algebraic number fields.* In Caviness B.F. (Ed.) EUROCAL '85. Lecture Notes in Computer Science 204, 289–290. Springer (1985). 2

[5] Demeyer F., Ingraham E. *Separable algebras over commutative rings.* Springer Lecture Notes in Mathematics 181 (1971). 4

[6] Díaz Toca G. *Galois Theory, Splitting fields and Computer Algebra.* à paraître Journal of Symbolic Computation (2005) 2

[7] Ducos L. *Effectivité en théorie de Galois. Sous-résultants.* Université de Poitiers, Thèse doctorale. Poitiers (1997). 11, 12

[8] Ducos L. *Construction de corps de décomposition grâce aux facteurs de résolvantes. (French) [Construction of splitting fields in favour of resolvent factors].* Communications in Algebra **28** n°2, 903–924 (2000). 13

[9] Ekedahl E., Laskov D. *Splitting algebras, symmetric functions ans Galois Theory.* Journal of Algebra and its Applications, **4** (1), (2005), 59–76. 11

[10] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988). 2, 16

Table des matières