L'algèbre de décomposition universelle (Universal Decomposition Algebra)

Gema M. Diaz-Toca Henri Lombardi Claude Quitté

Résumé

In this paper we present important properties of the Universal Decomposition Algebra of a polynomial over a commutative ring. Moreover, when the base ring is a field, we introduce new algorithms which make it possible to approach both splitting field of f and Galois group in a dynamic way without applying factorization algorithms.

Résumé

On donne les principales propriétés de l'algèbre de décomposition universelle d'un polynome sur un anneau commutatif. Dans le cas d'un corps on applique ces résultats pour un traitement constructif et dynamique du corps des racines et du groupe de Galois 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 $\mathbf{A} \xrightarrow{\rho} \mathbf{C}$.

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, 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 améliorons les résultats connus concernant les points fixes d'une algèbre de décomposition universelle (sous l'action de S_n).

Dans la section 5 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 une généralisation du résultat qui affirme que « l'algèbre de décomposition universelle se diagonalise elle-même lorsque le polynome est séparable » au cas d'un quotient de Galois.

Dans la section 6 nous généralisons un résultat donné séparément par P. Aubry et A. Valibouze ([1]) et par L. Ducos ([8]) sur la structure « triangulaire » des idéaux galoisiens.

Dans la section 7, pour étudier constructivement le « corps des racines » d'un polynome $f \in \mathbf{K}[T]$ (où $\mathbf{K}$ est un corps discret), 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]. Rappelons qu'en mathématiques constructives un ensemble est dit *discret* lorsqu'on dispose d'un test d'égalité pour ses éléments.

Remerciements. Nous remercions Thierry Coquand pour ses conseils judicieux.

1 Modules de Cauchy et base canonique

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

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

où $\mathcal{J}(f)$ est l'idéal donné par les fonctions symétriques élémentaires des X_i :

$$\alpha_1 = \sum_{i=1}^{n} X_i,\ \alpha_2 = \sum_{1\le i<j\le n} X_iX_j,\ \ldots,\ \alpha_n = \prod_{i=1}^{n} X_i\,,$$

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

L'algèbre de décomposition universelle peut être caractérisée par la propriété suivante.

Note 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 $\mathbf{A}$-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.

Le groupe S_n des permutations de $\{X_1, \ldots, X_n\}$ agit sur $\mathbf{A}[X_1, \ldots, X_n]$ 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.

Note 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 :

$$\begin{array}{rcl} f_1(X_1) & = & f(X_1) \\ f_{k+1}(X_1, \ldots, X_{k+1}) & = & \frac{f_k(X_1,\ldots,X_{k-1},X_k) - f_k(X_1,\ldots,X_{k-1},X_{k+1})}{X_k - X_{k+1}} \quad (1 \leq k \leq n-1) \end{array}$$

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

Lemme 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 $\mathcal{B}(f)$.*

Lemme 1.4. *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 $\mathrm{N}_{\mathbf{B}/\mathbf{A}}(z) = \mathrm{N}_{\mathrm{S}_n}(z)$.*

Démonstration. 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 une algèbre prégaloisienne

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 d'ordre 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 appelé un *atome*. Dans le cas d'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 $\mathrm{Stab}(F)$ le stabilisateur de F. Et si $H \subset G$, $\mathrm{Fix}(H) = E^H$ désigne la partie de E formée par les 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 $(\mathbf{A}, \mathbf{B}, \mathrm{S}_n)$ 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 système fondamental d'idempotents orthogonaux (sfio). Un idéal de $\mathbf{C}$ est dit *galoisien* lorsqu'il est engendré par l'idempotent complémentaire d'un idempotent galoisien.

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* $\mathbf{C}_1/\langle 1 - g_1\rangle \simeq \mathbf{C}/\langle 1 - g'\rangle$.

Démonstration. 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. □

3 Éléments galoisiens dans une algèbre de Boole

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

Lemme 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.

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.

Note 3.3. Soit G un groupe fini opérant sur une algèbre de Boole C discrète, $e \neq 0$ dans C, et $\{e_1, \ldots, e_k\}$ 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 $i \neq j \in \{1, \ldots, k\}$, $e_i e_j = 0$.

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

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.*

1. *Pour toute famille finie d'éléments de C il existe un élément galoisien e_1 (notons $(e_1, \ldots, e_k)$ son orbite) et tel que chaque élément 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 $h = \sum_{\sigma \in H/E} \sigma(e)$.*
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 $\mathcal{P}(G/E)$([1]).*

Démonstration. Nous montrons seulement 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

[1] 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.

ensemble fini $S = \{e_1, \ldots, e_k\}$ et C' est isomorphe à l'algèbre de Boole des parties finies de S : $C' = \{\sum_{i\in F} e_i | F \in \mathcal{P}(\{1, \ldots, k\})\}$. 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 $(e_1, \ldots, e_k)$ est un sfio et e_1 est galoisien. □

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 tels que : $\forall \sigma \in L$, $\alpha\sigma \in \bigcup_{\tau\in L} \tau S$.
Fin.

Sous les hypothèses du théorème 3.4 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 3.5. En outre on peut également calculer le stabilisateur de e_1 (la *nouvelle approximation du groupe de Galois*) « sans sortir du groupe ». 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.

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.

4 Points fixes de $\mathrm{Adu}_{\mathbf{A},f}$

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* $\mathbf{C} = \mathbf{B}$*).*

- *Un* $x \in \mathbf{C}$ *est inversible (resp. régulier) si et seulement si* $\mathrm{N}_{\mathbf{C}/\mathbf{A}}(x)$ *est inversible (resp. régulier) dans* $\mathbf{A}$*.*
- *Un* $x \in \mathbf{A}$ *est inversible (resp. régulier) dans* $\mathbf{C}$ *si et seulement si il est inversible (resp. régulier) dans* $\mathbf{A}$*.*

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* $J^2 = \operatorname{disc} f \in \mathbf{A}$.
3. *En particulier les propriétés suivantes sont équivalentes :*
   (a) $\operatorname{disc} f$ *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).*

Démonstration. Le point 1 est facile par récurrence sur n.
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 $\operatorname{Ann}(\Omega_{\mathbf{B}/\mathbf{A}})$ 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). □

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

Théorème 4.3. *Si* $\operatorname{Ann}_{\mathbf{A}}(\langle 2, \operatorname{di}(f)\rangle) = 0$ *et a fortiori si* $\operatorname{Ann}_{\mathbf{A}}(\langle 2, \operatorname{disc}(f)\rangle) = 0$ *on a* $\operatorname{Fix}(\mathrm{S}_n) = \mathbf{A}$.

Démonstration. Puisque $\langle 2, \operatorname{di}(f)^2\rangle = \langle 2, \operatorname{disc}(f)\rangle$ un élément qui annule $\langle 2, \operatorname{di}(f)\rangle$ annule a fortiori $\langle 2, \operatorname{disc}(f)\rangle$. 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 $\mathbf{B}_1 = \operatorname{Adu}_{\mathbf{A}_1,F}$, 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'écriure 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 $\operatorname{di}(f) = (-1)^{n-1}F(-x_1)\operatorname{di}(F)$ par un calcul direct et passons à la récurrence proprement dite.
Nous supposons que $\operatorname{Ann}_{\mathbf{A}}(\langle 2, \operatorname{di}(f)\rangle) = 0$. On en déduit que $\operatorname{Ann}_{\mathbf{A}_1}(\langle 2, \operatorname{di}(F)\rangle) = 0$, car si $b = \beta_0 + \beta_1 x_1 + \cdots + \beta_{n-1}x_1^{n-1} \in \mathbf{A}_1$ annule $\operatorname{di}(F)$, il annule $\operatorname{di}(f) = (-1)^{n-1}F(-x_1)\operatorname{di}(F)$,

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. □

Note 4.4. 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 $v = x_1^2x_2 + a_1x_1^2 + (a_1^2 + a_2)x_1 + a_2x_2 \neq 0$ 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.

5 Séparabilité de $\mathrm{Adu}_{\mathbf{A},f}$

Dans cette section on suppose que $\mathrm{disc}\, f$ est un élément **inversible** de $\mathbf{A}$.

Le lemme suivant comme moyen de prouver constructivement le théorème 5.2 a été suggéré par Thierry Coquand.

Lemme 5.1. *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 lemme 1.3 sont dans* $\mathrm{Ker}\, \phi$.

Démonstration. Nous donnons la preuve pour $n = 4$ et laissons le soin au lecteur de rédiger une preuve formelle par récurrence .
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 $y = a(x_1, x_2) + x_3c(x_1, x_2)$ 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 5.2. *1. 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.*

Démonstration. 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 théorème suivant s'applique en particulier pour l'algèbre de décomposition universelle $\mathbf{B}$.

Théorème 5.3. (diagonalisation d'un quotient de Galois d'une algèbre de décomposition universelle)
Soit e *un idempotent galoisien de* $\mathbf{B}$*,* G *son stabilisateur 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* $\sigma \in G$ *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.*

Démonstration. 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 $\mathrm{Ker}\,\phi_\sigma$ sont deux à deux comaximaux : $\mathrm{Ker}\,\phi_\sigma$ contient $y_i - u_{\sigma i}$, $\mathrm{Ker}\,\phi_\tau$ contient $y_i - u_{\tau i}$, 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. □

6 Structure triangulaire des idéaux galoisiens

Nous démontrons dans cette section un résultat donné dans [1] et [8] en le généralisant un peu : notre théorème 6.1. Notre méthode de preuve est différente car elle ne s'appuie pas sur l'existence d'une cloture algébrique, et le cadre est plus général puisque nous avons à la base un anneau commutatif presque arbitraire à la place d'un corps.

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.

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).

Théorème 6.1. *Soit $(\mathbf{A}, \mathbf{C}, G)$ une algèbre galoisienne avec*

- *$\mathbf{C} = \mathbf{A}[y_1, \dots, y_n]$,*
- *G opère sur $\{y_1, \dots, y_n\}$ 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 $G = G_0$, $G_i = \{\sigma \in G\,;\, \sigma(y_k) = y_k,\ \forall k \leq i\}$, $(i = 1 \dots, n)$, 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 :

- *$\mathbf{A}[y_1, \dots, y_i] = \operatorname{Fix}(G_i)$ et $G_i = \operatorname{Stp}(\mathbf{A}[y_1, \dots, y_i])$.*
- *$r_i(T)$ 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 $\mathbf{A}[X_1, \dots, X_i]$.

Démonstration. 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

A-module projectif de rang constant $|G|/|G_1|$. Les coefficients de $r_1(T)$ sont fixes par G, donc dans **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 **A** et que σ fixe tous les éléments de **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 **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 **A** zéro-dimensionnel. Alors $\mathbf{A}_1$ est libre sur **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 $\mathbf{C} = \mathbf{A}_1[y_2, \ldots, y_n]$ avec G_1 qui opère sur $\{y_2, \ldots, y_n\}$ et les $y_i - y_j$ inversibles. Tout le raisonnement précédent fonctionne à l'identique en remplaçant **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 **A** et $\mathbf{F} = \mathrm{Frac}\,\mathbf{A} = S^{-1}\mathbf{A}$. Remarquons que puisqu'un élément régulier de **A** est régulier dans **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 $sz \in \mathbf{A}[y_1]$: $sz = c_0 + c_1 y_1 + \cdots + c_{d_1-1} y_1^{d_1-1}$. 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 **A**. On a

$$szy_1^k = c_0 y_1^k + c_1 y_1^{k+1} + \cdots + c_{d_1-1} y_1^{k+d_1-1}.$$

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

$$s\sigma(zy_1^k) = c_0 y_\ell^k + c_1 y_\ell^{k+1} + \cdots + c_{d_1-1} y_\ell^{k+d_1-1}.$$

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 **A** et $s \sum_{\sigma \in G/G_1} \sigma(zy_1)^k = c_0 s_k + \cdots + c_{d_1-1} s_{k+d_1-1} \in s\mathbf{A}$. 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.

Nous terminons en vérifiant que $\mathbf{A}[y_1]$ vérifie bien l'hypothèse du théorème, ce qui permet de faire fonctionner la récurrence. En effet, puisque $\mathbf{A}[y_1]$ est libre sur **A** les éléments réguliers de **A** sont réguliers dans $\mathbf{A}[y_1]$ et l'anneau total des fractions de $\mathbf{A}[y_1]$

contient $\mathbf{F}[y_1] \simeq \mathbf{F}[X_1]/\langle r_1(X_1)\rangle$, lequel est zéro-dimensionnel, donc égal à son anneau total des fractions. □

Le théorème 6.1 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 $G = G_0 = \mathrm{St}(e) = \mathrm{St}(\mathfrak{b}) \subset \mathrm{S}_n$, 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 $\mathbf{A} = \mathrm{Fix}(G)$ 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 $i \neq j$.

7 Corps des racines

Dans cette section, nous remplaçons l'anneau $\mathbf{A}$ par un corps discret $\mathbf{K}$ 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.

Une $\mathbf{K}$-algèbre est dite *finie* si c'est un $\mathbf{K}$-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 $\mathbf{K}$-espace vectoriel de dimension finie.

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

7.1 f arbitraire

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 ne dispose pas toujours d'un tel idempotent. Le théorème suivant explique comment contourner la difficulté que pose la non existence du corps des racines en mathématiques constructives.

Théorème 7.1. *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 $\mathbf{B} \to \mathbf{B}_1$).*

Démonstration. Puisque $\mathbf{B}$ est zéro-dimensionnel on peut pour chaque $i \in I$ calculer un idempotent $g_i \in \mathbf{B}$ tel que 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. □

Le théorème d'unicité du corps des racines admet la version constructive suivante, qui découle du théorème 3.4 :

Théorème 7.2. *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 $\mathbf{C}_2 \simeq \mathbf{C}^{r_2}$.*

7.2 f séparable

Ici nous donnons une preuve constructive d'un résultat classique.

Notez que le rsultat fondamental suivant est obtenu sans utiliser le corps des racines (une approximation convenable de ce corps suffit).

Théorème 7.3. *Soit $\mathbf{K}$ un corps discret et $f \in \mathbf{K}[X]$ un polynome séparable. Alors l'algèbre de décomposition universelle $\mathbf{B} = \mathrm{Adu}_{\mathbf{K},f}$ est séparable (i.e., tout élément annule un polynome séparable de $\mathbf{K}[T]$).*

Démonstration. 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 7.1 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 4.3, 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 $P(z) \in \bigcap_i \langle 1-e_i\rangle = \langle 0\rangle$. □

Algorithme 7.4. **Calcul d'un idéal galoisien et de son stabilisateur.**

Entrée : $(\mathbf{C}, G)$: quotient de Galois de $(\mathbf{B}, \mathrm{S}_n)$, y : élément ni nul ni inversible de $\mathbf{C}$; $S = \mathrm{St}(y)$.
Sortie : $\mathfrak{c}$: idéal galoisien contenant y, et tel que tout conjugué de y sous G est nul ou inversible dans $\mathbf{C}/\mathfrak{c}$; H : le sous groupe stabilisateur de $\mathfrak{c}$.
Variables locales : $\mathfrak{a}$: idéal de C ; σ : dans G ; L : liste d'éléments de G.

Début
  $\mathfrak{c} \leftarrow < y >$; $L \leftarrow [\,]$;
  pour σ **dans** G/S **faire**
G/S désigne un système de représentants des classes à gauche modulo S
    $\mathfrak{a} \leftarrow \mathfrak{c} + < \sigma(y) >$;
    si $\mathfrak{a} \neq 1$ **alors** $\mathfrak{c} \leftarrow \mathfrak{a}$; $L \leftarrow L \bullet [\sigma]$ **fin si** ;
  fin pour
  $H \leftarrow$ le sous-groupe de G formé par les α tels que : $\forall \sigma \in L$, $\alpha\sigma \in \bigcup_{\tau \in L} \tau S$.
Fin.

L'algèbre $\mathbf{B} = \mathrm{Adu}_{\mathbf{K},f}$ est réduite quand le polynome f est séparable, donc tout idéal de type fini est engendré par un idempotent. Ce résultat implique qu'à partir d'un élément ni nul ni inversible y de $\mathbf{B}$ on peut calculer un idéal galoisien $\mathfrak{c}$ tel que $y \in \mathfrak{c}$ et tout conjugué de y sous S_n est nul ou inversible dans $\mathbf{B}/\mathfrak{c}$: $\mathfrak{c}$ est un idéal strict engendré par y et le plus grand nombre possible de conjugués de y.

En outre, le résultat reste le même si nous considérons une algèbre galoisienne $(\mathbf{K}, \mathbf{C}, G)$ qui est un quotient de Galois de $(\mathbf{K}, \mathbf{B}, \mathrm{S}_n)$.

Notons que l'algorithme 7.4 calcule un idéal galoisien $\mathfrak{c}$ engendré par un idempotent galoisien e_1 qui serait construit par l'algorithme 3.5 à partir d'un idempotent e tel que $(1-e)\mathbf{C} = y\mathbf{C}$. Ainsi $(\mathbf{C}/\mathfrak{c}, H)$ est une nouvelle approximation du corps de racines de f et de son groupe de Galois, meilleure que la précédente approximation $(\mathbf{C}, G)$.

Bibliographie

[1] Aubry P., Valibouze A. *Using Galois Ideals for Computing Relative Resolvents.* J. Symbolic Computation, **30**, 635–651, (2000). 2, 11

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

[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.* Universite de Poitiers, Thèse doctorale. Poitiers (1997). 9

[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** no. 2, 903–924 (2000). 2, 11

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

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

Gema M Díaz-Toca
Dpto. de Matemática Aplicada, Universidad de Murcia, Espagne
gemadiaz@um.es
Henri Lombardi
Laboratoire de Mathématiques de Besançon, Université de Franche-Comté, France
henri.lombardi@univ-fcomte.fr
Claude Quitté
Laboratoire de Mathématiques SP2MI, Université de Poitiers, France
claude.quitte@math.univ-poitiers.fr