CONSTRUCTION DE L'IDÉAL DES RELATIONS ENTRE LES RACINES D'UN POLYNÔME

Annick VALIBOUZE
LIP6, Université Paris VI, 4, place Jussieu, F-75252 Paris Cedex 05
e-mail : avb@medicis.polytechnique.fr

Résumé. Cette note développe une vision effective de la théorie de Galois algébrique en apportant des propriétés inhérentes aux idéaux associés à un polynôme d'une variable.

Computation of the ideal of the relations between the roots of a univariate polynomial

Abstract. *Galois theory allows us to deal with effective computation in algebraic extensions of fields. In this aim, the present paper is devoted to an effective inductive construction of an effective generator system for the ideal of relations between the roots of an univariate polynomial over a field. The idea is to define new ideals between the ideal of symmetric relations and the ideal of relations and to give a correspondance between these ideals and finite sets of permutations. The fundamental tools of this construction are multivariate polynomials called minimal polynomials associated to our ideals. These polynomials characterise the considered ideals and allow to construct a generators system for them.*

Introduction

La recherche du groupe de Galois d'un polynôme est motivée par l'étude de son corps de décomposition et par les manipulations des nombres algébriques qui lui appartiennent. La recherche du groupe de Galois peut-être remplacée par celle de l'idéal des relations entre les racines du polynôme. Dans [5] est proposé un algorithme de construction d'une base de Gröbner de cet idéal (voir [1] pour l'effectivité) ; il consiste à factoriser le polynôme dans des extensions successives du corps de base jusqu'au corps de décomposition. Cette note propose une méthode pour construire un système de générateurs de l'idéal des relations et ce sans factorisation dans des extensions. Sont définis des idéaux appelés *idéaux des relations invariantes par L*, où L est un ensemble de permutations (voir paragraphe 1.5). Puis est exhibé un polynôme caractérisant cet idéal et qui permet de construire explicitement un système de générateurs de cet idéal (voir paragraphe 2.2). Ensuite est établie une correspondance entre ces idéaux et des ensembles de permutations (voir paragraphe 2.3). Cette note termine sur le paragraphe 2.4 qui explique comment les outils introduits permettent de construire inductivement l'idéal des relations.

1. Définitions et notations préliminaires

1.1. **Les données.** Soient
- k un corps supposé parfait et $\hat{k}$ une clôture algébrique de k,
- f un polynôme d'une variable de degré n dont les coefficients appartiennent à k,
- $\Omega = (\alpha_1, \ldots, \alpha_n)$, où $\alpha_i \in \hat{k}$, un ensemble ordonné des racines du polynôme f,
- $x_1, \ldots, x_n$ des indéterminées (variables algébriquement indépendantes sur $\hat{k}$),
- $k[x_1, \ldots, x_n]$ l'anneau des polynômes en $x_1, \ldots, x_n$ à coefficients dans k et $k(x_1, \ldots, x_n)$ son corps des fractions.

1.2. **Action du groupe symétrique.** Prenons une fraction $\Theta \in k(x_1, \ldots, x_n)$.

Le **groupe symétrique de degré** n, noté $\mathfrak{S}_n$, agit naturellement sur le corps $k(x_1, \ldots, x_n)$. Pour $\sigma \in \mathfrak{S}_n$, l'action de σ sur Θ, notée $\sigma.\Theta$ ou $(\sigma.\Theta)$, est définie ainsi :

$$\sigma.\Theta(x_1, \ldots, x_n) = \Theta(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \qquad .$$

Soient L et H deux sous-groupes de $\mathfrak{S}_n$ tels que $H \subset L$. La fraction Θ est appelée un **H-invariant L-primitif** si Θ est un polynôme et $H = \{\sigma \in L \mid \Theta = \sigma.\Theta\}$.

Soit σ une permutation de $\mathfrak{S}_n$. L'action de σ sur Ω est définie naturellement par $\sigma.\Omega = (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$.

Soit $P \in k[x_1, \ldots, x_n]$. L'**évaluation de P en Ω** est le nombre algébrique $P(\Omega) = P(\alpha_1, \ldots, \alpha_n)$. La notation $\sigma.P(\Omega)$ n'est pas ambiguë : $\sigma.P(\Omega) = (\sigma.P)(\Omega)$. Néanmoins, le lemme suivant précise cette notation :

Lemme 1.1. *Soit $\sigma, \tau \in \mathfrak{S}_n$ et $P \in k(x_1, \ldots, x_n)$, alors $(\sigma.P)(\tau.\Omega) = P(\tau\sigma.\Omega)$.*

Soient L et H deux sous-groupes de $\mathfrak{S}_n$ tels que L contienne H et Θ un H-invariant L-primitif. Le polynôme Θ est dit **séparable pour** Ω si $H = \{\sigma \in L \mid \Theta(\Omega) = \sigma.\Theta(\Omega)\}$.

1.3. **Idéal des relations et groupe de Galois.** L'idéal I_Ω de $k[x_1, \ldots, x_n]$ défini par

$$I_\Omega = \{r \in k[x_1, \ldots, x_n] \mid r(\Omega) = 0\} \tag{1}$$

est connu sous le nom d'**idéal des relations (entre les racines du polynôme f)** et le **groupe de Galois de** f (relativement à Ω) est le sous-groupe G_Ω de $\mathfrak{S}_n$ défini par

$$G_\Omega = \{\sigma \in \mathfrak{S}_n \mid (\forall r \in I_\Omega)\ \sigma.r \in I_\Omega\} \qquad . \tag{2}$$

Le groupe de Galois G_Ω agit librement sur l'anneau quotient $A_{I_\Omega} := k[x_1, \ldots, x_n]/I_\Omega$ de la manière suivante :

$$\begin{array}{rcl} G_\Omega \times A_{I_\Omega} & \longrightarrow & A_{I_\Omega} \\ (\sigma, P) & \mapsto & \sigma.P(\Omega) = P(\sigma.\Omega) \qquad . \end{array}$$

Comme A_{I_Ω} est isomorphe à $k(\Omega)$, le corps de décomposition de f, cette action induit une action libre de G_Ω sur $k(\Omega)$. C'est ce qui, avec la correspondance galoisienne, rend essentiel la connaissance du groupe de Galois ou mieux encore celle de l'idéal I_Ω.

1.4. **Idéal invariant par un ensemble de permutations.**

Définition 1.2. Soit un sous-ensemble L de $\mathfrak{S}_n$, l'idéal

$$I_\Omega^L \quad = \quad \{r \in k[x_1, \ldots, x_n] \mid (\forall \sigma \in L)\ \sigma.r(\Omega) = 0\}$$

est appelé **idéal des Ω-relations invariantes par** L. En particulier l'idéal des relations, I_Ω, est l'idéal des relations invariantes par l'identité.

Si L contient l'identité nous avons : $I_\Omega^L = \{r \in I_\Omega \mid (\forall \sigma \in L)\ \sigma.r \in I_\Omega\} \subset I_\Omega$.

Notation 1.3. Nous notons $\mathrm{Max}(I_\Omega^L)$ le plus grand sous-ensemble du groupe symétrique $\mathfrak{S}_n$ qui vérifie :

$$I_\Omega^L = I_\Omega^{\mathrm{Max}(I_\Omega^L)} \qquad . \tag{3}$$

Définition 1.4. Le **groupe de décomposition de l'idéal** $I \subset k[x_1, \ldots, x_n]$, noté $\mathrm{Gr}(I)$, est défini par :

$$\mathrm{Gr}(I) = \{\sigma \in \mathfrak{S}_n \mid \sigma(I) = I\} \qquad . \tag{4}$$

2. Résultats

2.1. **Premières propriétés.** Il est évident que

$$G_\Omega = \mathrm{Max}(I_\Omega) = \mathrm{Gr}(I_\Omega) \quad \text{et} \tag{5}$$

$$\mathfrak{S}_n = \mathrm{Max}(I_\Omega^{\mathfrak{S}_n}) = \mathrm{Gr}(I_\Omega^{\mathfrak{S}_n}) \quad . \tag{6}$$

Les idéaux I_Ω et $I_\Omega^{\mathfrak{S}_n}$, appelé **idéal des relations symétriques (entre les racines de f)**, sont égaux ssi le groupe de Galois G_Ω est le groupe symétrique $\mathfrak{S}_n$.

Les propositions 2.1 et 2.2 montrent ce qu'il en est pour les idéaux I_Ω^L intermédiaires entre l'idéal des relations et l'idéal des relations symétriques.

Proposition 2.1. *Soit L un sous-groupe de $\mathfrak{S}_n$, nous avons :*

$$L \subset Gr(I_\Omega^L) \quad et \quad I_\Omega^{Gr(I_\Omega^L)} \subset I_\Omega^L \quad . \tag{7}$$

Proposition 2.2. *Soit I un idéal de $k[x_1, \ldots, x_n]$, si $I \subset I_\Omega$ alors $I \subset I_\Omega^{Gr(I)}$. En particulier, si $I = I_\Omega^L$, où L est un sous-groupe de $\mathfrak{S}_n$, alors*

$$I_\Omega^L = I_\Omega^{Gr(I)} = I_\Omega^{Max(I)} \tag{8}$$

et $L \subset Gr(I_\Omega^L) \subset Max(I_\Omega^L)$. Si, de plus, $Max(I_\Omega^L)$ est un groupe alors $Gr(I_\Omega^L) = Max(I_\Omega^L)$.

Désormais, nous considérons M et L deux sous-groupes du groupe symétrique $\mathfrak{S}_n$ tels que le groupe L et le groupe de Galois G_Ω soient inclus dans le groupe M. La situation est la suivante:

$$I_\Omega^{\mathfrak{S}_n} \subset I_\Omega^M \subset I_\Omega^L \subset I_\Omega \quad . \tag{9}$$

Nous nous donnons Θ un L-invariant M-primitif séparable pour Ω. Posons $\theta := \Theta(\Omega)$ et $R_{L,M} := \mathrm{Min}_{\theta,k}(\Theta)$ où $\mathrm{Min}_{\theta,k}$ est le polynôme minimal de θ sur k.

2.2. **Polynôme primitif.** Le théorème suivant exhibe un polynôme qui caractérise l'idéal I_Ω^L relativement à l'idéal I_Ω^M :

Théoreme 2.3.

$$R_{L,M} \in I_\Omega^L \quad ; \tag{10}$$

$$G_\Omega L = \{\sigma \in M \mid \sigma.R_{L,M}(\Omega) = 0\} \quad ; \tag{11}$$

$$Max(I_\Omega^L) = G_\Omega L \quad ; \tag{12}$$

$$I_\Omega^L = I_\Omega^M + (R_{L,M}) \quad . \tag{13}$$

Le polynôme $R_{L,M}$ du Théorème 2.3 est appelé **polynôme M-primitif de l'idéal I_Ω^L.**

2.3. **Correspondance entre idéaux et ensembles de permutations.** Nous aboutissons à cette correspondance entre les ensembles $\mathrm{Max}(I)$ et les idéaux de relations invariantes par des groupes :

Théoreme 2.4. *soit H un sous-groupe de $\mathfrak{S}_n$, alors $H \subset G_\Omega L$ ssi $I_\Omega^L \subset I_\Omega^H$. De plus, $H \subset G_\Omega L$ implique $Max(I_\Omega^H) = G_\Omega H \subset G_\Omega L$.*

2.4. **Construction de l'idéal des relations I_Ω.** Il s'agit de construire un système de générateurs de l'idéal I_Ω à partir de l'hypothèse inductive (9). Nous supposons connaître le polynôme $Min_{\theta,k}$ (lorsque les générateurs de I_Ω^M sont connus, cela est toujours possible par des calculs de résolvantes relatives ou de polynômes caractéristiques.) Au départ $M = \mathfrak{S}_n$.

L'idée naturelle est de poursuivre cette construction avec le Théorème 2.3. Il n'est pas possible de remplacer M par L, s'il ne contient pas G_Ω, ni par $G_\Omega L$, si ce n'est pas un groupe. Il s'agit donc d'exhiber un groupe qui contienne G_Ω et qui permette de poursuivre cette construction.

Soit $\tau_1, \ldots, \tau_r$ une transversale à gauche de $M \mod L$. Posons $\mathcal{O} := \{\tau_1.\Theta, \ldots, \tau_e.\Theta\}$ la G_Ω-orbite de Θ dans l'ensemble des $\tau_i.\Theta$ ($i \in [1, r]$) et $\mathcal{L} := \{\tau_1 L, \ldots, \tau_e L\}$, la G_Ω-orbite de L dans les classes à gauche de M mod L (en renumérotant éventuellement la transversale). Posons $S := \mathrm{Stab}_M(\mathcal{L}) = \mathrm{Stab}_M(\mathcal{O}) = \{\sigma \in M \mid (\forall i \in [1,e])\ \sigma.(\tau_i.\Theta) \in \mathcal{O}\}$. Les e nombres algébriques distincts $\tau_1.\Theta(\Omega), \dots, \tau_e.\Theta(\Omega)$ sont les conjugués de $\theta = \Theta(\Omega)$ sur k (voir [3]).

Proposition 2.5. *Si L est un groupe alors $G_\Omega \subset S \subset G_\Omega L$ et :*

$$I_\Omega^L = I_\Omega^{G_\Omega L} \subset I_\Omega^S \subset I_\Omega \quad . \tag{14}$$

De plus, $L \subset Gr(I_\Omega^L) \subset G_\Omega L$ et $S = Gr(I_\Omega^S) = G_\Omega S$ puisque $Max(I_\Omega^S) = S$ est un groupe.

Le groupe S qui contient le groupe de Galois G_Ω peut donc jouer le rôle du groupe M dans le Théorème 2.3. Mais pour ce faire, il faut calculer un polynôme M-primitif de l'idéal I_Ω^S. Il nous est donné par le Lemme suivant :

Lemme 2.6. *Soit $\Theta_{S,M}$ un M-invariant S-primitif séparable pour Ω. Alors $\Theta_{S,M}(\Omega)$ appartient à k et $\Theta_{S,M} - \Theta_{S,M}(\Omega)$ est un polynôme M-primitif de l'idéal I_Ω^S.*

Remarque 1. Dans [4], A. Colin propose de prendre pour $\Theta_{S,M}$ un polynôme symétrique en $\tau_1.\Theta, \dots \tau_e.\Theta$. Le Théorème fondamental des fonctions symétriques permet alors le calcul de $\Theta_{S,M}(\Omega)$ puisque les fonctions symétriques élémentaires en $\tau_1.\Theta(\Omega), \dots \tau_e.\Theta(\Omega)$ sont, à un signe près, les coefficients du polynôme minimal de $\theta = \Theta(\Omega)$ sur k qui est supposé connu.

Le test d'arrêt de notre construction est donné par la proposition suivante :

Proposition 2.7. *Il y a équivalence entre les trois assertions suivantes :*
(i) $G_\Omega = S = G_\Omega L$;
(ii) $L \subset G_\Omega$;
(iii) $I_\Omega = I_\Omega^M + (R_{L,M})$.
(L'équivalence entre (i) et (iii) a été démontrée dans [2] dans le cas où $S = \mathfrak{S}_n$.)

La proposition suivante place le cadre dans lequel $G_\Omega L = S$.

Proposition 2.8. *Il y a équivalence entre les 7 assertions suivantes :*
(1) $L \subset S$;
(2) $I_\Omega^L = I_\Omega^S = I_\Omega^{G_\Omega L}$;
(3) $G_\Omega L = S$ (il est toujours vrai que $G_\Omega S = S$) ;
(4) $G_\Omega L$ est un groupe (ou bien $L G_\Omega \subset G_\Omega L$) ;
(5) $Gr(I_\Omega^L) = G_\Omega L$;
(6) $S = Gr(I_\Omega^L)$;
(7) $G_\Omega \subset Gr(I_\Omega^L)$.
En particulier, quand $G_\Omega \subset L$ alors $G_\Omega \subset Gr(I_\Omega^L)$.

Conclusion. De l'étude des idéaux invariants par des permutations, a été exhibée une construction de l'idéal des relations sans avoir à factoriser dans des extensions de k. Pour que cette méthode soit réellement effective, il faut pouvoir calculer le polynôme minimal intervenant dans le paragraphe 2.4 et identifier le groupe S. Cela se fait en calculant des résolvantes et en étudiant les matrices des partitions qui permettent de calculer le groupe de Galois du polynôme (voir [2]).

References

[1] **Anai H., Noro M., Yokoyama K., 1994** Computation of the splitting field and the Galois groups of polynomials, Progress in Mathematics, 143 (conference MEGA'94), Birkhaüser Verlag, pp. 29–50.

[2] **Arnaudiès J.M., Valibouze A., 1993.** Résolvantes de Lagrange, Rapport LITP 93.61.

[3] **Arnaudiès J.M., Valibouze A., 1996.** Lagrange resolvents, *J. Pures Appl. Alg.* special issue of MEGA'96, eds. A. Cohen and M-F- Roy, à paraître.

[4] **Colin A., 1997** Identification of the Galois group thanks to symbolic computation of relative resolvents and tables of partitions, ISSAC'97 Conference (Haway, July 1997).

[5] **Tchebotarev N., 1950** *Grundzüge des Galois'shen Theorie* P. Noordhoff.