Théorie de Galois effective : aide mémoire

Annick Valibouze

THORIE DE GALOIS EFFECTIVE : AIDE MMOIRE

ANNICK VALIBOUZE

Cet article recense de nombreux rsultats obtenus dans diverses publications relevant de la thorie de Galois effective ; en particulier, les formules et thormes sur les idaux galoisiens peuvent s'exprimer de diverses façons et sont parfois "redcouverts" par de triviales reformalisations. L'parpillement complique galement leur utilisation rapide.

Les idaux galoisiens (dits alors de Galois) apparurent tout d'abord dans un support de cours et d'encadrement doctoral en thorie Galois effective (voir [14]) ; ce support comportant un nombre important de rsultats nouveaux servit galement de document de travail au projet Galois du GDR (puis de l'UMS) MEDICIS du CNRS.

Cet article a comme double objectif que 1) ne soient pas redcouverts des rsultats dj connus et 2) de les retrouver rapidement.

1. Donnes

- k un corps , $\overline{k}$ une clture algbrique de k
- $x_1, \ldots, x_n, x$ variables indpendantes sur k
- f polynme en x de degr n coefficients dans k
- $\alpha_1, \ldots, \alpha_n$ les n racines de f dans $\overline{k}$:

$$f = a_n \prod_{i=1}^{n} (x - \alpha_i) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

2. Notations gnrales

- $\mathfrak{S}_n$: groupe symtrique de degr n.
- I_n : sous-groupe identit de $\mathfrak{S}_n$
- A_n : sous-groupe altern de $\mathfrak{S}_n$

Date: December 15, 2010.

- $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n)$, $\boldsymbol{x} = (x_1, \ldots x_n)$, $\boldsymbol{a} = (a_1, \ldots, a_n)$, $\boldsymbol{i} = (i_1, \ldots, i_n)$, etc ...
- $\boldsymbol{x}^{\boldsymbol{i}} := x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$, etc ...
- $$pol(\boldsymbol{y}) := \prod_{i=1}^{n} (x - y_i)$$

3. Groupes

3.1 Gnralits classiques

$G, H \in \mathfrak{S}_n$

- $G < H$: G sous-groupe de H
- $G \subset H$: G sous-ensemble de H
- $GH = \{gh \mid \ g \in G \ h \in H\}$
- Hyp. $G < H$; $G_1, \ldots, G_s$ sont *les classes droite (resp. gauche) de H modulo G* si pour $i = 1, \ldots, s$, $G_i = G\tau_i$ (resp. $\sigma_i G$) o $\tau_i \in H$ (resp. $\sigma_i \in H$), et H est l'union disjointe des G_i :
$$H = G_1 + \cdots + G_s$$
- $G\backslash H := \{\tau_1, \ldots, \tau_s\}$ est une *transversale droite* de H modulo G.
- $H/G := \{\sigma_1, \ldots, \sigma_s\}$ est une *transversale gauche* de H modulo G.
- $[H : G] := s$, l'*indice* de G dans H
- G est un sous-groupe *distingu* (*normal*) de H si $G < H$ et
$$(\forall \tau \in H)\ G = \tau G \tau^{-1}$$
(i.e. les classes droite et gauche sont identiques)
- $G^\tau := \tau G \tau^{-1}$
- G sous-groupe distingu de H ssi la tranversale (droite et gauche) de H modulo G forme un sous-groupe de H not H/G (=$G\backslash H$)
- *Action (gauche)* de G, un groupe, sur un ensemble non vide E, toute opration note $\star$:
$$\mathfrak{S}_n \times E \longrightarrow \quad E, \quad (\sigma, x) \mapsto \sigma \star x$$
vrifiant les axiomes suivants :

(1) $(\forall x \in E)$, $e_G \star x = x$, o e_G est l'lment neutre de G

(2) $(\forall x \in E)\,, (\forall \sigma, \tau \in \mathfrak{S})$, $\sigma \star (\tau \star x) = (\sigma\tau) \star x$

- $x \in E$, $\sigma \in G$:

$$\begin{array}{rcl} \sigma \star E & := & \{\sigma \star x \mid x \in E\} \\ G \star x & := & \{\sigma \star x \mid \sigma \in G\} \quad \textit{orbite de } x \textit{ sous l'action de } G \\ G \star E & := & \{G \star x \mid x \in E\} = \{\sigma \star E \mid \sigma \in G\} \\ \mathrm{Stab}_G\, x & := & \{\sigma \in G \mid \sigma \star x = x\} \quad \textit{stabilisateur de } x \textit{ dans } G \end{array}$$

3.2 Actions particulires

Soit $\sigma \in \mathfrak{S}_n$.

- $\mathfrak{S}_n$ agit naturellement sur $E := \{1, \ldots, n\}$ comme groupe de permutations :

$$\mathfrak{S}_n \times E \longrightarrow E, \quad (\sigma, j) \mapsto \sigma(j) = i_j \quad \text{si } \sigma = \begin{pmatrix} 1, \ldots, n \\ i_1, \ldots, i_n \end{pmatrix}$$

- $\mathfrak{S}_n$ agit sur les n-uplets :

$$\sigma * \boldsymbol{y} := (y_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

- $\mathfrak{S}_n$ agit sur les monmes :

$$\sigma.\boldsymbol{x}^{\boldsymbol{i}} := (\sigma * \boldsymbol{x})^{\boldsymbol{i}} = x_{\sigma(1)}^{i_1} x_{\sigma(2)}^{i_2} \cdots x_{\sigma(n)}^{i_n}$$

  et par extension $\mathfrak{S}_n$ agit sur $k(\boldsymbol{x})$.

- (plus tard) $\mathrm{Gal}_k(\boldsymbol{\alpha})$ agit sur $k(\boldsymbol{\alpha})$:
  $\Theta \in k[\boldsymbol{x}]$, $\theta = \Theta(\alpha_1, \ldots, \alpha_n) \in k(\boldsymbol{\alpha})$, $\tau \in \mathrm{Gal}_k(\boldsymbol{\alpha})$,

$$\beta^\tau = \Theta(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)})$$

  Rq : $\mathrm{Gal}_k(\boldsymbol{x}) = \mathfrak{S}_n$ agit sur $k(\boldsymbol{x})$; on pourrait noter $p^\sigma := \sigma.p$, $p \in k(\boldsymbol{x})$

- (plus tard) $\mathrm{Gal}_k(f) := \mathrm{Aut}_k(k(\boldsymbol{\alpha}))$ agit sur $k(\boldsymbol{\alpha})$:

$$\mathrm{Gal}_k(f) \times k(\alpha) \longrightarrow k(\alpha), \quad (\phi, \beta) \mapsto \phi(\beta)$$

- Notation : $r \in k[\boldsymbol{x}]$,

$$\sigma.r(\boldsymbol{\alpha}) := (\sigma.r)(\boldsymbol{\alpha}) = r(\sigma * \boldsymbol{\alpha})$$

- $(\forall \sigma, \tau \in \mathfrak{S}_n)$, $(\forall r \in k[\boldsymbol{x}])$,

$$\tau\sigma.r(\boldsymbol{\alpha}) = r(\tau\sigma * \boldsymbol{\alpha}) = \sigma.r(\tau * \boldsymbol{\alpha})$$

  (i.e. permuter d'abord r avec σ puis valuer en $\tau * \boldsymbol{\alpha}$)

3.3 Matrices des groupes et de partitions

Soient $G, H < L < \mathfrak{S}_n$. Soit $\mathcal{O}$ l'ensemble des G-orbites de L modulo H. Pour tout $O \in \mathcal{O}$ de cardinal s, on note $Gr(G, O)$, la reprsentation symtrique dans $\mathfrak{S}_s$ de l'action gauche de G sur O ; soit le vecteur de groupes

$$Gr_L(G, H) := [Gr(G, O) \mid O \in \mathcal{O}]$$

- $Gr_L(G, H)$ ne dpend pas de la classe de conjugaison de G et H dans $\mathfrak{S}_n$
- $\mathcal{G}(L)$ *matrice des groupes de* L
  elle est indice en colonne et en ligne par les classes de conjugaison des sous-groupes de S_n - Soient G, H deux sous-groupes de S_n ; l'intersection de la ligne de la classe de H et de la colonne de celle de G se trouve le vecteur de groupes $Gr_L(G, H)$.
- $\mathcal{P}(L)$ *matrice des partitions de* L
  c'est la matrice dduite de $\mathcal{G}(L)$ en remplaant les groupes par leur degr respectif.
- Les lignes de la matrice de partitions (et donc de groupes) sont toutes distinctes.

4. Idaux galoisiens

4.1 Gnralits classiques

I idal de $k[\boldsymbol{x}]$, $V \subset \overline{k}^n$

- idal dfinit par V dans $k[\boldsymbol{x}]$:
  $$\mathrm{Id}_{k[\boldsymbol{x}]}(V) := \{r \in k[\boldsymbol{x}] \mid (\forall \boldsymbol{b} \in V)\ r(\boldsymbol{b}) = 0\}$$
  (par dfaut $\mathrm{Id}(V) := \mathrm{Id}_{k[\boldsymbol{x}]}(V)$)
- idal engendr par $r_1, \ldots, r_m \in k[\boldsymbol{x}]$ dans $k[\boldsymbol{x}]$:
  $$< r_1, \ldots, r_m >_{k[\boldsymbol{x}]} := \{u_1 r_1 + \cdots + u_m r_m \mid u_1, \ldots, u_m \in k[\boldsymbol{x}]\}$$
  (par dfaut $< r_1, \ldots, r_m > := < r_1, \ldots, r_m >_{k[\boldsymbol{x}]}$)
- $r \in k[\boldsymbol{x}]$: idal monogne $rk[\boldsymbol{x}] := < r >_{k[\boldsymbol{x}]}$
- I *maximal* dans $k[\boldsymbol{x}]$ si $(\forall r \in k[\boldsymbol{x}] - I)\ I + < r >= k[\boldsymbol{x}]$
- I_1, I_2 *comaximaux* si $I_1 + I_2 = k[\boldsymbol{x}]$
- I *radical* si $r^m \in I \Rightarrow r \in I$

- I, J idaux de $k[\boldsymbol{x}]$; *injecteur de I dans J* :
$$\mathrm{Inj}(I,J) := \{\sigma \in \mathfrak{S}_n \mid \ \sigma.I \subset J\}$$
- si $V := V(I)$ est finie alors

(1) $$\dim_k(k[\boldsymbol{x}]/\mathrm{Id}(V)) = \mathrm{Card}(V)$$

- si $V(I)$ est finie alors $k[\boldsymbol{x}]/I$ est engendr par les monmes sous l'escalier d'un base de Gröbner de I pour l'ordre lexicographique.

4.2 Idaux galoisiens : notations et dfinitions

- tout idal galoisien est radical
- $H \subset \mathfrak{S}_n$, l'*idal galoisien $I^H_{\boldsymbol{\alpha}}$ dfini par H et $\boldsymbol{\alpha}$* :
$$I^H_{\boldsymbol{\alpha}} \ := \ \{r \in k[\boldsymbol{x}] \mid (\forall \sigma \in H)\ \sigma.r(\boldsymbol{\alpha}) = 0\}$$

- $I_{\boldsymbol{\alpha}} := I^{I_n}_{\boldsymbol{\alpha}}$
- *idal des $\boldsymbol{\alpha}$-relations* : $\mathfrak{M} := \{r \in k[\boldsymbol{x}] \mid r(\boldsymbol{\alpha}) = 0\} = I_{\boldsymbol{\alpha}}$
- *idal des relations symtriques* : $\mathfrak{S} := I^{\mathfrak{S}_n}_{\boldsymbol{\alpha}}$; ne dpend pas du choix de $\boldsymbol{\alpha}$.
- Autres faons de voir l'idal galoisien $I^H_{\boldsymbol{\alpha}}$ dfinit par H et $\boldsymbol{\alpha}$:
$$\begin{aligned} I^H_{\boldsymbol{\alpha}} &= \{r \in k[\boldsymbol{x}] \mid (\forall \sigma \in H)\ r(\sigma * \boldsymbol{\alpha}) = 0\} \\ &= \mathrm{Id}(H * \boldsymbol{\alpha}) \\ &= \{r \in k[\boldsymbol{x}] \mid (\forall \sigma \in H)\ \sigma.r \subset \mathfrak{M}\} \end{aligned}$$

  (on pourra noter $I^H_{\mathfrak{M}} := I^H_{\boldsymbol{\alpha}}$).
- Attention : si $I_n \not\subset H$ alors $I^H_{\boldsymbol{\alpha}} \not\subset \mathfrak{M} = I_{\boldsymbol{\alpha}}$

4.3 Ensembles de permutations particuliers

- *groupe de dcomposition de I* (aussi $\mathrm{Stab}_{S_n}(I)$) : $Gr(I) = \mathrm{Inj}(I,I)$
- $\mathrm{Max}(I, \boldsymbol{\alpha})$: *plus grand ensemble de permutations dfinissant $I^H_{\boldsymbol{\alpha}}$ avec $\boldsymbol{\alpha}$*
- *groupe de Galois de $\boldsymbol{\alpha}$ sur k* :

(2) $$Gal_k(\boldsymbol{\alpha}) := Gr(\mathfrak{M}) \ = \ \mathrm{Max}(\mathfrak{M}, \boldsymbol{\alpha})$$

(3) $$= \ \{\sigma \in \mathfrak{S}_n \mid \ r(\boldsymbol{\alpha}) = 0 \Rightarrow \sigma.r(\boldsymbol{\alpha}) = 0\}$$

4.4 Idaux galoisiens purs

I est dit *pur* si $\mathrm{Max}(I, \boldsymbol{\alpha})$ est un groupe.

Nous retrouverons ces idaux galoisiens plus loin.

4.5 Premires proprits

I, J, I_i idaux galoisiens, $G, H \subset \mathfrak{S}_n$, $\sigma, \tau \in \mathfrak{S}_n$, $\mathfrak{M} = I_{\boldsymbol{\alpha}}$

- $\mathfrak{M}$ est un idal maximal de $k[\boldsymbol{x}]$
  $(r(\boldsymbol{\alpha}) = 0 \Rightarrow (\forall \sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})), \sigma.r(\boldsymbol{\alpha}) = 0 \Rightarrow r \in \mathfrak{M})$
- Cette proprit et la suivante sont exprimes sous une autre forme dans 4.6
$$I^H_{\sigma * \boldsymbol{\alpha}} = I^{\sigma H}_{\boldsymbol{\alpha}}$$
- $$\sigma . I^H_{\boldsymbol{\alpha}} = I^{H\sigma^{-1}}_{\boldsymbol{\alpha}}$$
- C.P. $I_{\sigma * \boldsymbol{\alpha}} = \sigma^{-1}.I_{\boldsymbol{\alpha}} = \sigma^{-1}.\mathfrak{M}$
- $\mathcal{G}$ un ensemble d'ensembles de permutations (i.e. inclus dans les parties de $\mathfrak{S}_n$) ;
$$I^{\bigcup_{G \in \mathcal{G}}}_{\boldsymbol{\alpha}} = \bigcap_{G \in \mathcal{G}} I^G_{\boldsymbol{\alpha}}$$
- $$\begin{aligned} \mathrm{Max}(I, \boldsymbol{\alpha}) &= \mathrm{Inj}(I, \mathfrak{M}) = \{\sigma \in \mathfrak{S}_n \mid \ r \in I \Rightarrow \sigma.r(\boldsymbol{\alpha}) = 0\} && (4)\\ &= \mathrm{Gal}_k(\boldsymbol{\alpha}) H && (5)\\ &= \bigcup_{G \subset \mathfrak{S}_n \mid I = I^G_{\boldsymbol{\alpha}}} G && (6) \end{aligned}$$
- $$I \subset I^{\mathrm{Gr}(I)}_{\boldsymbol{\alpha}} \quad (\forall \boldsymbol{\alpha} \in V(I))$$
- si H est un groupe alors
$$I^H_{\boldsymbol{\alpha}} = I^{\mathrm{Gr}(I^H_{\boldsymbol{\alpha}})}_{\boldsymbol{\alpha}}$$
  et
$$H \subset \mathrm{Gr}(I^H_{\boldsymbol{\alpha}}) \subset Max(I^H_{\boldsymbol{\alpha}}, \boldsymbol{\alpha})$$
- $\mathrm{Max}(I, \boldsymbol{\alpha})$ est un groupe (i.e. I est pur) si et seulement si l'une des conditions suivantes est satisfaite

(i) $\mathrm{Gal}_k(\boldsymbol{\alpha}) < Gr(I)$

(ii) $Gr(I) = \mathrm{Max}(I, \boldsymbol{\alpha})(= \mathrm{Inj}(J, \mathfrak{M}))$

(iii) $Gr(I) = \mathrm{Inj}(I, J)$ pour tout idal J contenant I

- $(\forall \beta \in V(I))$, $\sigma \notin \mathrm{Max}(I, \boldsymbol{\beta})$ si et seulement si
$$I + \sigma.I = k[\boldsymbol{x}]$$
(quivalent : pour tout idal maximal $\mathfrak{M}'$ contenant I, $\sigma \notin \mathrm{Inj}(I, \mathfrak{M}')$)
- $\mathfrak{S}_n = Gr(\mathfrak{S}) = \mathrm{Max}(\mathfrak{S}, \boldsymbol{\alpha})$
- **Correspondance galoisienne inhrente aux idaux galoisiens**

(i) $G \subset H \subset \mathfrak{S}_n \Rightarrow I_{\boldsymbol{\alpha}}^H \subset I_{\boldsymbol{\alpha}}^G$

(ii) $\mathfrak{S} \subset \mathcal{I} \subset \mathcal{J} \subset \mathfrak{M} = I_{\boldsymbol{\alpha}} \Rightarrow \mathcal{I}, \mathcal{J}$ sont galoisiens et
$$\mathfrak{S}_n \subset \mathrm{Max}(\mathcal{I}, \boldsymbol{\alpha}) \subset \mathrm{Max}(\mathcal{J}, \boldsymbol{\alpha}) \subset \mathrm{Gal}_k(\boldsymbol{\alpha})$$

- Comme $\mathfrak{M} = I_{\boldsymbol{\alpha}}^{I_n} = I_{\boldsymbol{\alpha}}^{\mathrm{Gal}_k(\boldsymbol{\alpha})}$ et $\mathrm{Gal}_k(\boldsymbol{\alpha}) = Gr(\mathfrak{M}) = \mathrm{Max}(\mathfrak{M}, \boldsymbol{\alpha})$,
$$(\forall H \subset \mathrm{Gal}_k(\boldsymbol{\alpha})), \quad I_{\boldsymbol{\alpha}}^H = I_{\boldsymbol{\alpha}}^{\mathrm{Gal}_k(\boldsymbol{\alpha})}$$

4.5 Autres faon d'exprimer $I \subset I_{\boldsymbol{\alpha}} = \mathfrak{M}$

- $$\begin{aligned} I &= \bigcap_{\sigma \in \mathrm{Max}(I, \boldsymbol{\alpha})} I_{\sigma * \boldsymbol{\alpha}} \\ &= \bigcap_{\sigma \in \mathrm{Inj}(I, \mathfrak{M})} \sigma^{-1}.\mathfrak{M} \end{aligned}$$
- $\mathfrak{S} \subset I \subset J \Rightarrow \bigcap_{\sigma \in \mathrm{Inj}(I,J)} \sigma^{-1}.J \subset I$
- $\mathfrak{S} \subset I \subset J \subset \mathfrak{M}$, $H = \mathrm{Max}(I, \boldsymbol{\alpha})$, $G = \mathrm{Max}(J, \boldsymbol{\alpha})$ t.q.
$$H = G\tau_1 + \ldots + G\tau_s \qquad (*)$$
alors
$$I = \bigcap_{i=1}^{s} \tau_i^{-1}.J \tag{7}$$
(on peut montrer que la condition $(*)$ est toujours satisfaite)

- C.P. $G = \mathrm{Gal}_k(\boldsymbol{\alpha})$. Soient $\tau_1, \ldots, \tau_s$ t.q. $\mathrm{Max}(I, \mathfrak{M}) = G\tau_1 + \ldots + G\tau_s$ alors

$$I = \bigcap_{i=1}^{s} \tau_i^{-1}.\mathfrak{M} \quad (= \bigcap_{i=1}^{s} I_{\tau_i.\boldsymbol{\alpha}}) \tag{8}$$

- C.P. Soit $\tau_1 = id, \ldots, \tau_s$ transversale droite de $\mathfrak{S}_n$ modulo $\mathrm{Gal}_k(\boldsymbol{\alpha})$.

$$\mathfrak{S} = \mathfrak{M} \cap \tau_2^{-1}.\mathfrak{M} \cap \cdots \cap \tau_s^{-1}.\mathfrak{M} \quad (= I_{\boldsymbol{\alpha}} \cap I_{\tau_2.\boldsymbol{\alpha}} \cap \cdots \cap I_{\tau_s.\boldsymbol{\alpha}}) \tag{9}$$

- Soit $\mathcal{E}$ un ensemble d'idaux galoisiens

$$I = \bigcap_{J \in \mathcal{E}} J \Rightarrow \mathrm{Gr}(I) = \bigcap_{J \in \mathcal{E}} \mathrm{Inj}(I, J)$$

4.6 Quelques proprits des injecteurs

-

$$\mathrm{Inj}(\sigma.I, \tau.J) = \tau\, \mathrm{Inj}(I, J)\sigma^{-1} \tag{10}$$

- C.P. $\mathrm{Gal}_k(\sigma.\boldsymbol{\alpha}) = \mathrm{Inj}(\sigma^{-1}.\mathfrak{M}, \sigma^{-1}.\mathfrak{M}) = \sigma^{-1}\, \mathrm{Gal}_k(\boldsymbol{\alpha})\sigma$
- $H\, \mathrm{Inj}(I, \mathfrak{M}) = \mathrm{Inj}(.I, \mathfrak{M}) \Rightarrow H\, \mathrm{Inj}(G.I, \mathfrak{M}) = \mathrm{Inj}(G.I, \mathfrak{M})$
- $\mathfrak{S} \subset I_i \subset J$, $i = 1, 2$;

$$\mathrm{Inj}(I_1 + I_2, J) = \mathrm{Inj}(I_1, J) \cap \mathrm{Inj}(I_2, J) \tag{11}$$

- $\mathfrak{S} \subset I \subset J_i$, $i = 1, 2$;$\mathrm{Inj}(I, J_1 \cap J_2) = \mathrm{Inj}(I, J_1) \cap \mathrm{Inj}(I, J_2)$
- $H \subset \mathfrak{S}_n$, $L := \mathrm{Inj}(I, J)$;

$$\mathrm{Inj}(H.I, J) = \bigcap_{h \in H} Lh^{-1} \text{ et } \mathrm{Inj}(I, H.J) = \bigcap_{h \in H} hL$$

- $\mathrm{Inj}(J, \mathfrak{M})\, \mathrm{Inj}(I, J) \subset \mathrm{Inj}(I, \mathfrak{M})$
- Soit un polynme f de degr n et I un idal galoisien de f d'injecteur un groupe H. L'ensemble des idaux galoisiens de f d'injecteur H est form des $\sigma.I$ o σ parcourt le normalisateur de H dans S_n.

5. Varits

5.1 Gnralits classiques

I, I_1, I_2 idaux de $k[\boldsymbol{x}]$

- varit de I : $V(I) := \{\boldsymbol{\beta} \in \overline{k}^n \mid (\forall r \in I)\ r(\boldsymbol{\beta}) = 0\}$
- $V(\mathrm{Id}(V(I))) = V(I)$
- $I = I_1 \cap I_2 \Rightarrow V(I) = V(I_1) \cup V(I_2)$
- I_1, I_2 comaximaux $\Leftrightarrow V(I_1) \cap V(I_2) = \{\ \}$
- I radical $\Leftrightarrow I = \mathrm{Id}(V(I))$
- I_1, I_2 radicaux ; $V(I) = V(I_1) \cup V(I_2) \Rightarrow I = I_1 \cap I_2$

5.2 Idaux galoisiens

I idal galoisien

- $$V(I) = Max(I, \boldsymbol{\alpha}) \star \boldsymbol{\alpha} \tag{12}$$
- C.P. $V(\mathfrak{S}) = \mathfrak{S}_n \star \boldsymbol{\alpha} \quad et \quad V(\mathfrak{M}) = Gal_k(\boldsymbol{\alpha}) \star \boldsymbol{\alpha}$

La varit d'un idal galoisien peut s'exprimer trivialement sous forme de varits disjointes ds lors que l'on exprime $Max(I, \boldsymbol{\alpha})$ sous forme de classes droite disjointes $G_{\boldsymbol{\alpha}}\tau$ et que f est sans racine multiple.

6. Anneaux quotients, Varites, Idaux galoisiens et Injecteurs

Ce paragraphe doit tre considr avec attention pour concevoir qu'un mme rsultat peut s'exprimer de nombreuses façons selon qu'on l'exprime avec les varits, les injecteurs, les anneaux quotients ou les idaux galoisiens et/ou en modifiant lgrement les hypothses pour lui donner une apparence de nouveaut.

$I = I^L_{\boldsymbol{\alpha}}$, on a $Max(I, \boldsymbol{\alpha}) = G_{\boldsymbol{\alpha}}\tau_1 + \cdots + G_{\boldsymbol{\alpha}}\tau_s$, $\tau_i \in L$ (on peut toujours supposer que $L = Max(I, \boldsymbol{\alpha})$). Un idal galoisien d'un polynme sans racine multiple est radical. Notre polynme f est suppos sans racine multiple.

- $$\dim_k(k[\boldsymbol{x}]/I) = \mathrm{Card}(V(I)) = \mathrm{Card}(Max(I, \boldsymbol{\alpha}))$$

- C.P. idal de $\boldsymbol{\alpha}$-relations :

$$k[\boldsymbol{x}]/\mathfrak{M} \equiv k(\boldsymbol{\alpha})$$

et

$$\dim_k(k[\boldsymbol{x}]/\mathfrak{M}) = \mathrm{Card}(\mathrm{Gal}_k(\boldsymbol{\alpha}))$$

- C.P. idal des relations symtriques

$$\dim_k(k[\boldsymbol{x}]/\mathfrak{S}) = n!$$

Soient $V_1, \ldots, V_s$ des varits incluses dans $V(I)$ et $L_1, \ldots, L_s$ les ensembles maximaux de permutations tels que $V_i = L_i.\boldsymbol{\alpha}$ (i.e. $L_i = G_{\boldsymbol{\alpha}} = Max(Id(V_i), \boldsymbol{\alpha})$).

L'ensemble $V(I)$ est l'union disjointe des varits $V_1, \ldots, V_s$ ssi les ensembles de permutations $L_1, \ldots, L_s$ sont deux--deux disjoints et (union disjointe)

$$Max(I, \boldsymbol{\alpha}) = L_1 + \cdots + L_s;$$

dans ce cas, puisque les $I_i := Id(V_i)$ sont deux--deux comaximaux et que $I = \bigcap_{i=1}^{s} I_i$, il vient (thorme des restes chinois) :

$$k[\boldsymbol{x}]/I = \prod_{i=1}^{s} k[\boldsymbol{x}]/I_i$$

En particulier, soient $\tau_1, \ldots, \tau_s$ (deux--deux distincts) tels que (union disjointe)

$$Max(I, \boldsymbol{\alpha}) = G_{\boldsymbol{\alpha}}\tau_1 + \cdots + G_{\boldsymbol{\alpha}}\tau_s;$$

comme $I_i = \tau_i^{-1}.\mathfrak{M}$ en posant $I_i = \mathfrak{M}_i$, un idal maximal conjugu de $\mathfrak{M}$,

$$k[\boldsymbol{x}]/I = \prod_{i=1}^{s} k[\boldsymbol{x}]/\mathfrak{M}_i \equiv k(\boldsymbol{\alpha})^s$$

7. Polynmes multivaris particuliers

- $e_0(\boldsymbol{y}) = 1, e_1(\boldsymbol{y}), \ldots, e_r(\boldsymbol{y}), \ldots$, les *fonctions symtriques lmentaires* en $\boldsymbol{y} := (y_1, \ldots, y_n)$:

$$\begin{array}{lll} e_r(\boldsymbol{y}) := & \sum_{m \in \mathfrak{S}_n.(y_1 \cdots y_r)} m & \text{si } 1 \leq r \leq n \\ e_r(\boldsymbol{y}) := & 0 & \text{si } n < r \end{array}$$

$e_1(\boldsymbol{y}) = y_1 + \cdots + y_n$, $e_2(\boldsymbol{y}) = y_1y_2 + y_1y_3 + \cdots + y_{n-1}y_n$, $\ldots$, $e_n(\boldsymbol{y}) = y_1y_2 \cdots y_n$.

- $p_0(\boldsymbol{y}) = n, p_1(\boldsymbol{y}), \ldots, p_r(\boldsymbol{y}), \ldots$, les *fonctions puissances* (de Newton) en $\boldsymbol{y} := (y_1, \ldots, y_n)$:

$$p_r(\boldsymbol{y}) := \sum_{i=1}^{n} y_i^r \qquad (\forall r \in \mathbb{N})$$

- $h_0(\boldsymbol{y}) = 1, h_1(\boldsymbol{y}), \ldots, h_r(\boldsymbol{y}), \ldots$, les *fonctions compltes* en $\boldsymbol{y} := (y_1, \ldots, y_n)$:

$$h_r(\boldsymbol{y}) := \sum_{i_1+\cdots+i_n=r} \boldsymbol{y}^{\boldsymbol{i}} \qquad (\forall r \in \mathbb{N})$$

- $e_r := e_r(\boldsymbol{x})$, $p_r := p_r(\boldsymbol{x})$,..., $\widetilde{e_r} = e(\boldsymbol{\alpha})$,...
- *formules de Girard-Newton* : pour tout $m \geq 0$

$$p_m e_0 - p_{m-1} e_1 + \cdots + (-1)^{m-1} p_1 e_{m-1} + (-1)^m m.e_m = 0 \quad . \tag{13}$$

- **Polynme** $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ **:**

$$\frac{f}{a_n} = x^n - e_1(\boldsymbol{\alpha}) x^{n-1} + e_2(\boldsymbol{\alpha}) x^{n-2} + \cdots + (-1)^n e_n(\boldsymbol{\alpha})$$

- *formules de Girard-Newton* : $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$; pour tout $m \geq 0$

$$\widetilde{p_m} a_0 + \widetilde{p_{m-1}} a_1 + \cdots + \widetilde{p_1} a_{m-1} + m.a_m = 0 \quad . \tag{14}$$

o $a_i = 0$ si $i > n$.

- $C_1(f), \ldots, C_n(f)$, *les modules de Cauchy de* f dans $k[\boldsymbol{x}]$: posons $C_i := C_i(f)$

$$\begin{aligned} C_1(x_1) &:= f(x_1) \\ C_2(x_1, x_2) &:= \frac{C_1(x_1) - C_1(x_2)}{x_1 - x_2} \\ &\vdots \\ C_r(x_1, \ldots, x_r) &:= \frac{C_{r-1}(x_1, \ldots, x_{r-2}, , x_{r-1}) - C_{r-1}(x_1, \ldots, x_{r-2}, , x_r)}{x_{r-1} - x_r} \quad 1 < r \leq n \end{aligned}$$

-

$$C_{r+1} = \sum_{i=r}^{n} a_i h_{i-r}(x_1, x_2, \ldots, x_r) \quad r = 0, \ldots, n-1 \tag{15}$$

- EX. $f := x^4 - 2x^3 + 2x^2 + 2$

$$\begin{aligned} C_1(x_1) &= x_1^4 - 2x_1^3 + 2x_1^2 + 2 \\ C_2(x_1, x_2) &= x_2^3 + x_1x_2^2 + x_1^2x_2 + x_1^3 - 2(x_2^2 + x_1x_2 + x_1^2) + 2(x_2 + x_1) \\ C_3(x_1, x_2, x_3) &= x_3^2 + x_3x_2 + x_2^2 + x_3x_1 + x_2x_1 + x_1^2 - 2(x_2 + x_1 + x_3) + 2 \\ C_4(x_1, x_2, x_3, x_4) &= x_4 + x_3 + x_2 + x_1 - 2 \quad . \end{aligned}$$

8. Polynmes caractristiques, minimaux et rsolvantes

Gnralits classiques

$\Theta \in k[\boldsymbol{x}]$, I idal de $k[\boldsymbol{x}]$

- *endomorphisme multiplicatif induit* par Θ dans $k[\boldsymbol{x}]/I$:

$$\hat{\Theta} : k[\boldsymbol{x}]/I \longrightarrow \quad k[\boldsymbol{x}]/I, \quad \overline{p} \mapsto \hat{\Theta}(\overline{p}) = \overline{\Theta.p}$$

- $C_{\Theta,I}$, $M_{\Theta,I}$: polynmes caractristique et minimal de $\hat{\Theta}$
- si k parfait alors $M_{\Theta,I}$ est la forme sans facteur carr de $C_{\Theta,I}$
- si I radical alors

$$C_{\Theta,I} = \prod_{\boldsymbol{\beta} \in V(I)} (x - \Theta(\boldsymbol{\beta})) \tag{16}$$

Hypothses

$H \subset L \subset \mathfrak{S}_n$, $I = I_{\boldsymbol{\alpha}}^L$, $L = Max(I, \boldsymbol{\alpha})$, $\Theta \in k[\boldsymbol{x}]$, $H = \mathrm{Stab}_L(\Theta)$.

Invariants

- Θ est un *H-invariant L-primitif* si $H = \mathrm{Stab}_L(\Theta)$
  on pourra lire relatif la place de primitif
- Soit $K = k(e_1, \ldots, e_n)$. Θ est l'lment un *H-invariant L-primitif* ssi Θ est un lment K-primitif de $K(\boldsymbol{x})^H$ sur $K(\boldsymbol{x})^L$
- dans MAGMA : `RelativeInvariant` dans GAP : `PrimitiveInvariant`
- Θ est un H-invariant L-primitif *$\boldsymbol{\alpha}$-sparable* si pour tout $\sigma \in L$

$$\sigma.\Theta \neq \sigma.\Theta \Rightarrow \sigma.\Theta(\boldsymbol{\alpha}) \neq \tau.\Theta(\boldsymbol{\alpha})$$

- soit M un sous-groupe de L ; alors tout H-invariant L-primitif est aussi un H-invariant M-primitif
- tout H-invariant L-primitif $\boldsymbol{\alpha}$-sparable est aussi un H-invariant M-primitif $\boldsymbol{\alpha}$-sparable
- f sans racine multiple ; il existe toujours un H-invariant $\mathfrak{S}_n$-primitif $\boldsymbol{\alpha}$-sparable pour tout sous-groupe H de $\mathfrak{S}_n$
- un H-invariant L-primitif est dit *universel* s'il est toujours $\boldsymbol{\alpha}$-sparable pour tout n-uplet $\boldsymbol{\alpha}$ constitu de valeurs deux--deux distinctes
- EX. le Vandermonde $\prod_{1\leq i<j\leq n}(x_i - x_j)$ est un A_n-invariant $\mathfrak{S}_n$-primitif universel.
- $\boldsymbol{i} \in \mathbb{N}^n$; un H-invariant (on peut prendre aussi une combinaison linaire) :

$$\Psi_{\boldsymbol{i},H} := \sum_{\sigma\in H}(\sigma \star \boldsymbol{x})^{\boldsymbol{i}}$$

- si les parts de $\boldsymbol{i}$ sont deux--deux distinctes alors $\Psi_{\boldsymbol{i},H}$ est $\mathfrak{S}_n$-primitif (car $\sigma.(H.\boldsymbol{x}^{\boldsymbol{i}}) = H.\boldsymbol{x}^{\boldsymbol{i}} \Leftrightarrow \sigma \star (H \star \boldsymbol{x}) = H \star \boldsymbol{x} \Leftrightarrow \sigma H = H$)
- $\sigma \in L$; si Θ H-invariant L-primitif alors $\sigma.\Theta$ est un H^σ-invariant L-primitif

Rsolvantes

- $G \subset \mathfrak{S}_n$, $\Theta \in k[\boldsymbol{x}]$, *rsolvante G-relative de $\boldsymbol{\alpha}$ par Θ* :

$$R_{\Theta,G,\boldsymbol{\alpha}} := \prod_{\Psi\in G.\Theta}(x - \Psi(\boldsymbol{\alpha}))$$

  (on peut prendre $\Theta \in k(\boldsymbol{x})$ si aucun dnominateur des polynmes de $G.\Theta$ n'appartient $\mathfrak{M}$; i.e. il ne s'annule pas en $\boldsymbol{\alpha}$)
- on peut noter $R_{\Theta,I} := R_{\Theta,\mathrm{Max}(I,\boldsymbol{\alpha}),\boldsymbol{\alpha}}$
- une rsolvante L-relative de $\boldsymbol{\alpha}$ par Θ est appele une *H-rsolvante L-relative de $\boldsymbol{\alpha}$*
- $$C_{\Theta,I} = R_{\Theta,I}^{\#H}$$
- si k corps parfait alors $R_{\Theta,I} \in k[\boldsymbol{x}]$

- si $L = \tau_1 H + \cdots + \tau_e H$ alors
$$R_{\Theta,I} = \prod_{i=1}^{e} (x - \tau_i.\Theta(\boldsymbol{\alpha}))$$

- Θ est un H-invariant L-primitif $\boldsymbol{\alpha}$-*sparable* si et seulement si $R_{\Theta,I}$ est sans racine multiple (i.e. $i \neq j \Rightarrow \tau_i.\Theta(\boldsymbol{\alpha}) \neq \tau_j.\Theta(\boldsymbol{\alpha})$) ; dans ce cas $R_{\Theta,I}$ est la forme sans facteur carre de $C_{\Theta,I}$, le polynme caractristique de $\hat{\Theta}$, et si, de plus, k est parfait alors $R_{\Theta,I} = M_{\Theta,I}$, le polynme minimal de $\hat{\Theta}$.

- Soit $K = k(e_1, \ldots, e_n)$. La rsolvante gnrique $R_{\Theta,L,\boldsymbol{x}}$ est le polynme minimal de Θ sur $K(\boldsymbol{x})^L$

- Tout facteur h k-irrductible de $R_{\Theta,I}$ est naturellement le polynme minimal de chacune de ses racines sur k ;

- (k parfait) si h est un facteur k-irrductible de multiplicit 1 de la rsolvante $R_{\Theta,I}$ et ne possdant aucune racine multiple alors chacune de ses racines $\sigma.\Theta(\boldsymbol{\alpha})$ est un lment primitif de $k(\boldsymbol{\alpha})^{G_{\boldsymbol{\alpha}} \cap H^\sigma}$ sur $k(\boldsymbol{\alpha})^{G_{\boldsymbol{\alpha}} \cap L}$ o $G_{\boldsymbol{\alpha}}$ est le groupe de Galois de $\boldsymbol{\alpha}$ sur k (ici $k(\boldsymbol{\alpha})^{G_{\boldsymbol{\alpha}} \cap L} = k(\boldsymbol{\alpha})^{G_{\boldsymbol{\alpha}}} = k$ puisque $G_{\boldsymbol{\alpha}} \subset L$, par hypothse.

- h est un facteur simple sur k de la rsolvante $R_{\Theta,I}$ ssi Θ est un H-invariant $G_{\boldsymbol{\alpha}}$-primitif $\boldsymbol{\alpha}$-sparable

- Pour toutes les subtilits concernant les facteurs des rsolvantes (simples, non simples, k parfait ou non parfait) voir [18]

- pour tudier les rsolvantes avec les classes doubles : voir [21]

9. Gnrateurs des idaux galoisiens

Hypothses :
I idal galoisien, $\boldsymbol{\alpha} \in V(I)$, f sans racine multiple, k corps parfait (si $g \in k[\boldsymbol{x}]$ est irrductible alors g est sans racine multiple)

-
$$\mathfrak{S} = < e_1 - \widetilde{e_1}, \ldots, e_1 - \widetilde{e_1} > \quad (17)$$
$$= < C_1, \ldots, C_1 > \quad (18)$$

- **Thorme de l'lment primitif sur les idaux galoisiens**

  Un polynme R est dit *J-primitif de l'idal I* si $J = I + < R >$.

I idal galoisien, $L = Max(I, \boldsymbol{\alpha})$, $H \subset L$, Θ un H-invariant L-primitif $\boldsymbol{\alpha}$-sparable alors

$$I_{\boldsymbol{\alpha}}^{H} = I + < h(\Theta) > \tag{19}$$

o h est le facteur simple de $R_{\Theta,I}$ tel que $h(\Theta(\boldsymbol{\alpha})) = 0$

- (version effective) Soit h un facteur simple de $R_{\Theta,I}$ et $\boldsymbol{\beta}$ tel que $h(\Theta(\boldsymbol{\beta})) = 0$ alors

$$I_{\boldsymbol{\beta}}^{H} = I + < h(\Theta) > \tag{20}$$

- **Racines multiples de la rsolvante** : le thorme de l'lment primitif et l'usage des matrices de groupes se gnralisent. Consulter l'article [18] dans lequel un exemple concret conclut partir d'un facteur multiple de la rsolvante.

  Ci-aprs une partie des rsultats relve de l'article [4].

- $\{f_1, \ldots, f_n\} \in k[\boldsymbol{x}]$ est un *ensemble triangulaire* si pour tout $i \in [\![1, n]\!]$, le polynme f_i est de degr au minimum 1 en x_i et s'exprime sous la forme :
$$f_i = x_i^{deg_{x_i}(f_i)} + g(x_1, \ldots, x_i)$$

- un ensemble triangulaire $\{f_1, \ldots, f_n\}$ est dit *sparable* si f_1 est sans racine multiple pour tout $i \in [\![2, n]\!]$ et pour tout $\boldsymbol{\beta} \in V(< f_1, \ldots, f_{i-1} >)$, $f_i(\beta_1, \ldots, \beta_{i-1}, x)$ est sans racine multiple.

- si I est pur et f sans racine multiple alors il existe un ensemble triangulaire sparable engendrant I ; cet ensemble forme une base de Gröbner de I pour l'ordre lexicographique :
$$I =< f_1, \ldots, f_n >;$$

- $\mathrm{Init}(I) := (\deg_{x_1}(f_1), \ldots, \deg_{x_n}(f_n))$: n-uplet constitu des *degrs initiaux* de I

- $H \subset \mathfrak{S}_n$, $H_{(0)} := H$, $H_{(i)} := Stab_{H_{(i-1)}}(i)$, $i = 1, \ldots n$

- $\mathrm{Gal}_k(\boldsymbol{\alpha}) < H = \mathrm{Gr}(I)$ (i.e. I pur), $(\forall i \in [\![1, n]\!])$,

$$(\forall \boldsymbol{\beta} \in V(I)) \quad f_i(\beta_1, \ldots, \beta_{i-1}, x) = \prod_{\tau \in H_{(i-1)}/H_{(i)}} (x - \beta_{\tau(i)})$$

(gnralisable tout idal galoisien triangulaire)

- $\mathrm{Gal}_k(\boldsymbol{\alpha}) < H = \mathrm{Gr}(I)$ (i.e. I pur), pour tout $i \in [\![1, n]\!]$; alors

$$\deg_{x_i}(f_i) = \frac{\#H_{(i-1)}}{\#H_{(i)}}$$

- I triangulaire, $\mathrm{Init}(I) = (m_1, \cdots, m_n)$, degrs initiaux ;

$$k[\boldsymbol{x}]/I =< \boldsymbol{x^i} \mid \ 0 \leq i_1 < m_1, \ldots 0 \leq, i_n < m_n >$$

- I galoisien triangulaire ;

$$\begin{aligned} \dim_k(k[\boldsymbol{x}]/I) &= \mathrm{Card}(V(I)) \\ &= \mathrm{Card}(\mathrm{Max}(I, \boldsymbol{\alpha})) \\ &= \prod_{i=1}^{n} \deg_{x_i}(f_i) \end{aligned} \tag{21}$$

- si $I = \mathfrak{M} =< f_1, \ldots, f_n >$ ($\mathfrak{M}$ est pur) o les f_i sont appels les *modules fondamentaux* par Tchebotarev.

- Chaque module fondamental f_i est le polynme minimal de α_i sur $k(\alpha_1, \ldots, \alpha_{i-1})$.

L'objectif de la thorie de Galois effective (et donc du projet Galois) est de calculer l'idal des relations $\mathfrak{M}$ et le groupe de Galois $\mathrm{Gr}(\mathfrak{M})$, son groupe de dcomposition (un groupe de dcomposition est facilement calculable), c'est--dire le corps de dcomposition de f avec l'action du groupe de Galois sur ses racines.

Pour ce faire, il faut utiliser toutes les mthodes pour calculer des facteurs dans les extensions ou bien calculer une base de Gröbner d'un idal maximal : incluant et combinant de l'interpolation multivarie (voir [7], [10]) avec du numrique, du modulaire, ...), de l'algbre linaire (avec du numrique, du p-adique : [23] et [22], du modulaire), des rsolvantes, des matrices de groupes, la construction d'une chane ascendante d'idaux galoisiens, ...; on peut supposer connatre un idal I (dfaut l'idal des relations symtriques) et chercher un seul idal de sa dcomposition en idaux premiers (ils sont tous conjugus) en utilisant les injecteurs pour acclrer et orienter les calculs (voir [11]). Les informations, mme partielles, sur le groupe de Galois sont exploitables pour viter de nombreuses tapes de calculs, voir pour calculer directement $\mathfrak{M}$.

Et pour tout dire, il faut mlanger toutes les mthodes pour produire un algorithme parallle et collaboratif.

Il convient nanmoins de concevoir que les stratgies sont distinctes des techniques de calcul. Par exemple, l'interpolation multivarie peut se raliser en modulaire ou en numrique. L'interpolation multivarie tant elle-mme une technique de calcul reposant sur des informations galoisiennes. L'objectif d'tablir une formule exprimant les "sparateurs" (i.e. les polynmes jouant le rle des polynmes de Lagrange en univari) dans le cas d'un idal galoisien connaissant son injecteur ; dans le cas $I = \mathfrak{M}$ pour [7] restreint aux modules fondamentaux $f_i(\alpha_1, \ldots, \alpha_{i-1}, x)$ linaires en x pour [10].

Nous avons dsormais des outils simples et extrmement efficaces : par exemple, permuter une relation peut produire un module fondamental ou un lment primitif d'un idal galoisien ; cette permutation est prvisible avant l'excution du programme (voir Section sur les idaux galoisiens purs ou bien [12], [19] et [8]). Ce qui signifie que les calculs sont dans ces cas instantans. Un autre cas de calculs rapides et prvisibles : il suffit de diviser certains gnrateurs de $\mathfrak{M}$ par d'autres pour obtenir immdiatement de nouveaux. Les exemples donns dans [12] illustrent l'efficacit de ces deux techniques. Cette mthode inclut celle consistant calculer des modules de Cauchy de certains f_i pour en dduire d'autres (voir [8]). Il est facile de reformuler ces mthodes en modifiant le contexte sans rien apporter de nouveau pour le calcul effectif.

10. Idaux galoisiens purs

Rappelons que I est dit *pur* si $\mathrm{Max}(I, \boldsymbol{\alpha})$ est un groupe.

Par dfinition : $Gr(I) = Stab_{S_n}(I) = \mathrm{Inj}(I, I)$ et $\mathrm{Max}(I, \boldsymbol{\alpha}) = \mathrm{Inj}(I, \mathfrak{M})$.

On peut toujours se ramener un idal galoisien pur lorsque les constructions d'idaux galoisiens sont ralises partir de groupes (ce qui est le cas en pratique) (voir [21]) :

Si H et E sont deux sous-groupes de $\mathfrak{S}_n$ tels que $\mathrm{Inj}(I, \mathfrak{M}) = HE$ et que H est un tel groupe qui est maximal dans $\mathrm{Inj}(I, \mathfrak{M})$ alors $H.I$ est un idal galoisien pur de groupe de dcomposition H.

Le groupe H existe toujours puisque si $I = I^E_{\boldsymbol{\alpha}}$ alors $\mathrm{Inj}(I, \mathfrak{M}) = G_{\boldsymbol{\alpha}}E$, $G_{\boldsymbol{\alpha}}$, groupe de Galois de $\boldsymbol{\alpha}$ sur k.

Le choix du nombre minimal de permutations de H suffisantes au calcul de $H.I$ (en effectif, les permutations portent sur les gnrateurs de I) est tudi dans [12] et [8] offre une tude pratique en degr 8. Prvoir ces permutations est pr-calculable groupistiquement (c'est ce qui a t fait pour l'tude de cas dans [8]).

Si un idal galoisien est pur alors il est triangulaire (voir [4]).

Nous avons dans ce qui prcde de nombreuses conditions ncessaires et suffisantes pour qu'un idal galoisien soit pur. Nous les rcapitulons ici. Les conditions suivantes sont quivalentes

(1) I est pur

(2) $\mathrm{Max}(I, \boldsymbol{\alpha})$ est un groupe

(3) $\mathrm{Gal}_k(\boldsymbol{\alpha}) < Gr(I)$

(4) $Gr(I) = \mathrm{Max}(I, \boldsymbol{\alpha})$

(5) $Gr(I) = \mathrm{Inj}(I, J)$ pour tout idal J contenant I (si c'est vrai pour $\mathfrak{M}$, c'est vrai pour tous)

(6)
$$\dim_k(k[\boldsymbol{x}]/I) = \mathrm{Card}(\mathrm{Stab}_{S_n}(I))$$

(7)
$$\mathrm{Card}(V(I)) = \mathrm{Card}(\mathrm{Stab}_{S_n}(I))$$

(8)
$$\prod_{i=1}^{n} \deg_{x_i}(f_i) = \mathrm{Card}(\mathrm{Stab}_{S_n}(I))$$

11. Corps des racines

Thorie (presque)-classique

Gnralits classiques : rappels

- Si K est un corps, une **extension** L/K est une K-algbre L qui est un corps.
- on note $[L : K] := dim_K L$ et on dit que L/K est *finie* si $[L : K]$ est finie et *triviale* si $[L : K] = 1$.
- un lment de L est dit *algbrique* sur K s'il est racine d'un polynme coefficients dans K.
- si tout lment de L/K est algbrique alors L/K est dite *algbrique*
- $\gamma \in L$, le *polynme minimal* $\min_{\gamma,K}$ de γ sur K est l'unique polynme unitaire coefficients dans K tel que $\min_{\gamma,K}(\gamma) = 0$
- On dit que $\gamma \in L$ est *sparable* sur K si $\mathrm{diff}(\min_{\gamma,K}, x)(\gamma) \neq 0$; i.e. $\min_{\gamma,K}$ ne possde pas de racine multiple.

- Une extension algbrique L/K est *sparable* si tout $\gamma \in L$ est sparable sur K.
- On dit que $P \in K[x]$ se *dcompose* sur une extension L/K en produit de facteurs linaires s'il existe $c \in K$ et $u_1, \ldots, u_d \in L$ avec $P = c(x-u_1)\ldots(x-u_d)$
- l'extension L est appele un *corps de dcomposition* pour P si, en plus, $L = K(u_1, ..., u_d)$
- On dit aussi qu'un polynme non-constant $P \in K[x]$ est *sparable* (ou sans racine multiple) s'il se dcompose sur un corps de dcomposition en produit de facteurs linaires distincts (i.e. ses racines sont deux--deux distinctes).
- $\gamma \in L$ est sparable sur K si et seulement si $\min_{\gamma,K}$ est sparable.
- Un *corps de rupture* pour $P \in K[x]$ est une extension L/K telle qu'il existe $\gamma \in L$ avec $P(\gamma) = 0$ et $L = K(\gamma)$.
- Si L/K est une extension et $\gamma \in L$, alors $K(\gamma)$ est un corps de rupture pour $\min_{\gamma,k}$ sur K.
- un corps est dit **parfait** si toutes ses extensions finie sont sparables
- **Thorme de l'lment primitif (Lagrange)**
  Si L/K est une extension sparable finie alors il existe $\gamma \in L$ tel que $L = K(\gamma)$
- Un corps $\overline{K}$ est *algbriquement clos* s'il n'existe pas d'extension algbrique non-triviale de K. Une clture algbrique d'un corps K est une extension algbrique $\overline{K}/K$ qui est un corps algbriquement clos.
- Une extension algbrique L/K est dite *normale* si tout $P \in K[x]$ irrductible avec une racine dans L se dcompose en produit de facteurs linaires.
- Une extension finie est normale si et seulement si c'est le corps de dcomposition d'un polynme.
- Une extension algbrique L/K est dite **galoisienne** si elle est normale et sparable. (i.e. si pour le polynme minimal de tout lment de L se dcompose sur L en produit de facteurs linaires distincts.)

Corps de dcomposition de f

Hypothses : k corps parfait et f sparable (i.e. sans racine multiple)

Une *extension galoisienne de* k est le corps des racines (de dcomposition) d'un polynme coefficients dans k.

- **Corps des racines et idal maximal**
- $k(\boldsymbol{\alpha})$ est le corps des racines (de dcomposition) de f : corps des fractions de l'anneau $k[\boldsymbol{\alpha}]$, l'ensemble des combinaisons linaires finies sur k des $\boldsymbol{\alpha}^{\boldsymbol{i}}$ o $\boldsymbol{i} \in \mathbb{N}^n$; c'est une extension galoisienne
- morphisme surjectif d'valuation :
$$k[\boldsymbol{x}] \longrightarrow k[\boldsymbol{\alpha}], \quad p \mapsto p(\boldsymbol{\alpha})$$
de noyau $\mathfrak{M}$, idal maximal.
- corps $k[\boldsymbol{x}]/\mathfrak{M}$ est isomorphe $k[\boldsymbol{\alpha}]$; donc
$$k(\boldsymbol{\alpha}) = k[\boldsymbol{\alpha}] \simeq k[\boldsymbol{x}]/\mathfrak{M}$$
-
$$dim_k k(\boldsymbol{\alpha}) = \dim_k(k[\boldsymbol{x}]/\mathfrak{M}) = \mathrm{Card}(\mathrm{Gal}_k(\boldsymbol{\alpha})) \tag{22}$$
- $\mathrm{Gal}_k(f)$**, Groupe de Galois de** f
- $\mathrm{Gal}_k(f) := \mathrm{Aut}_k(k(\boldsymbol{\alpha}))$ groupe des automorphismes de $k(\boldsymbol{\alpha})$ (ensemble des k-endomorphismes bijectifs de $k(\boldsymbol{\alpha})$) ; $\phi \in \mathrm{Gal}_k(f)$ est entirement dtermin par une bijection de $\{\alpha_1, \ldots, \alpha_n\}$ dans lui-mme.
- isomorphisme de groupes
$$\mathrm{Gal}_k(\boldsymbol{\alpha}) \longrightarrow \mathrm{Gal}_k(f), \quad \sigma \mapsto \phi_\sigma$$
o pour $i \in [\![1, n]\!]$ $\quad \phi_\sigma(\alpha_i) = \alpha_{\sigma(i)}$
- $\sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})$, $\gamma \in k(\boldsymbol{\alpha})$, $\gamma^\sigma := \phi_\sigma(\gamma)$
- **Attention !** $\sigma \notin \mathrm{Gal}_k(\boldsymbol{\alpha})$;
(i) la notation γ^σ n'a aucun sens
(ii) $\gamma := \sum_{\boldsymbol{i}} \lambda_{\boldsymbol{i}} \boldsymbol{\alpha}^{\boldsymbol{i}} \in k(\boldsymbol{\alpha})$; l'galit $\gamma = 0$ ne peut en aucun cas impliquer que $\sum_{\boldsymbol{i} \in E} \lambda_{\boldsymbol{i}} (\sigma * \boldsymbol{\alpha})^{\boldsymbol{i}}$ soit nul ; c'est justement au groupe de Galois qu'appartient le pouvoir d'assurer cette implication pour ses lments ; il en va de mme pour $\gamma = \gamma'$ puisque $\gamma - \gamma' = 0$.
- **Corps de rupture et polynme minimal**
- le *polynme minimal de* $\gamma \in k(\boldsymbol{\alpha})$ *sur* k est le polynme, not $\min_{\gamma,k}$, irrductible sur k dont γ est racine

- Corps de rupture de $\gamma \in k(\boldsymbol{\alpha})$:
$$k(\gamma) = k[\gamma] \simeq k[\boldsymbol{x}]/ < \min_{\gamma,k} >$$

- $d := \deg_x(\min_{\gamma,k})$;
$$\gamma^0, \gamma^1, \ldots, \gamma^{d-1}$$
est une base de k-ev de $k(\gamma)$;
$$\dim_k(k(\gamma)) = d$$

- les *conjugus* de γ sur k sont les racines de son polynme minimal sur k.
- les conjugus de γ sur k sont les lments la $\mathrm{Gal}_k(\boldsymbol{\alpha})$-orbite de γ :
$$\min_{\gamma,k} = \prod_{\theta \in \{\gamma^\sigma \mid \sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})\}} (x - \theta)$$

- **Sous-Groupes de** $\mathrm{Gal}_k(f)$ **et sous-corps de** $k(\boldsymbol{\alpha})$
- $H < \mathrm{Gal}_k(\boldsymbol{\alpha})$, $k(\boldsymbol{\alpha})^H := \{\gamma \in k(\boldsymbol{\alpha}) \mid \ (\forall \gamma \in H), \gamma^\tau = \gamma\}$
- $H < \mathrm{Gal}_k(f)$, $k(\boldsymbol{\alpha})^H := \{\gamma \in k(\boldsymbol{\alpha}) \mid \ (\forall \phi \in H), \phi(\gamma) = \gamma\}$
- (Evariste Galois) Soit $\gamma \in k(\boldsymbol{\alpha})$; alors
$$(\forall \tau \in \mathrm{Gal}_k(\boldsymbol{\alpha})), \gamma^\tau = \gamma \Leftrightarrow \gamma \in k$$
dit autrement :
$$k(\boldsymbol{\alpha})^{\mathrm{Gal}_k(f)} = k$$

- $$k(\boldsymbol{\alpha})^{I_n} = k(\boldsymbol{\alpha})$$

- **Correspondance galoisienne (Artin)**
(i) K un corps ;
$$k \subset K \subset k(\boldsymbol{\alpha}) \Rightarrow (\exists H \subset \mathrm{Gal}_k(f)), \quad K = k(\boldsymbol{\alpha})^H$$
(ii) $H \subset \mathrm{Gal}_k(f) \Rightarrow k \subset k(\boldsymbol{\alpha})^H \subset k(\boldsymbol{\alpha})$

  cette correspondance dcrit une bijection entre les sous-groupes du groupe de Galois $\mathrm{Gal}_k(f)$ et les corps intermdiaires entre k et $k(\boldsymbol{\alpha})$.

- un groupe H est un sous-groupe distingu de $\mathrm{Gal}_k(f)$ si et seulement si l'extension $k(\boldsymbol{\alpha})^H$ de k est galoisienne

Phnomne extension-contraction : corps et idaux galoisiens

la correspondance galoisienne inhrente aux idaux galoisiens porte sur les **sur-ensembles** (et donc sur les sur-groupes) du groupe de Galois $Gal_k(\boldsymbol{\alpha})$ alors que la correspondance galoisienne classique inhrente aux corps (Artin) porte sur les **sous-groupes** de $Gal_k(\boldsymbol{\alpha})$ (ou bien $\mathrm{Gal}_k(f)$) ;
soit

$$H < Gal_k(\boldsymbol{\alpha}) < G \quad ;$$

nous avons
(i) H dcrit un corps intermdiaire entre k et $k(\boldsymbol{\alpha})$ tandis que sur les idaux

$$I_{\boldsymbol{\alpha}}^H = \mathfrak{M} = I_{\boldsymbol{\alpha}}^{Gal_k(\boldsymbol{\alpha})}$$

(ii) soit $K := k(e_1, \ldots, e_n)(\boldsymbol{x})^G$, le corps invariant par G (voir plus bas) ; G dcrit un idal intermdiaire entre $\mathfrak{S}$ et $\mathfrak{M}$ tandis que sur les corps

$$\widetilde{K} = k = k(\boldsymbol{\alpha})^{Gal_k(\boldsymbol{\alpha})}$$

(le $\tilde{}$ symbolise la spcialisation qui envoie x_i sur α_i).

C'est--dire que pour les idaux, les sous-ensembles de $Gal_k(\boldsymbol{\alpha})$ sont associs au mme idal, i.e. $\mathfrak{M}$, alors que pour les corps, les sur-groupes de $Gal_k(\boldsymbol{\alpha})$ sont associs au mme corps, i.e. k.

Nous pouvons voir cela encore autrement avec les k-algbres $A_G := k[\boldsymbol{x}]/I_{\boldsymbol{\alpha}}^G$. Posons $G_{\boldsymbol{\alpha}} := \mathrm{Gal}_k(\boldsymbol{\alpha})$:

$$(23)\ k = k(\boldsymbol{\alpha})^{G_{\boldsymbol{\alpha}}} = k(\boldsymbol{\alpha})^{G_{\boldsymbol{\alpha}} \cap G} \subset k(\boldsymbol{\alpha})^H \subset k(\boldsymbol{\alpha})^{I_n} \begin{array}{l} = \ k(\boldsymbol{\alpha}) \\ \simeq \ A_{G_{\boldsymbol{\alpha}}} = A_H \subset A_G \subset A_{\mathfrak{S}_n} \end{array}$$

- **extensions intermdiaires**
- Notation : $K_2 < K_1$ signifie K_1/K_2, le corps K_1 est une extension de K_2 ; i.e. K_1, K_2 corps et $K_2 \subset K_1$
- $k < K_2 < K_1 < k(\boldsymbol{\alpha})$ le *degr* $[K_1 : K_2]$ de K_1 sur K_2 est sa dimension en tant que K_2-espace vectoriel (rappel)

- $H_1 < H_2 < \mathrm{Gal}_k(f)$; l'indice de H_1 dans H_2 et le degr de $k(\boldsymbol{\alpha})^{H_1}$ sur $k(\boldsymbol{\alpha})^{H_2}$ sont identiques :
$$[H_2 : H_1] == [K_1 : K_2]$$
- extensions $K_3 < K_2 < K_1$
$$[K_1 : K_3] = [K_1 : K_2][K_2 : K_3]$$
- Soit $k < K_2 < K_1 < k(\boldsymbol{\alpha})$; γ est un lment K_2-*primitif de* K_1 si $K_1 = K_2(\gamma)$
- γ est un lment K_2-primitif de K_1 si et seulement si
$$\deg_x(\min_{\gamma,k}) = [K1 : K2]$$

Polynme gnrique

$$pol(\boldsymbol{x}) := \prod_{i=1}^{n}(x - x_i) = x^n - e_1x^{n-1} + \cdots + (-1)^n e_n$$

- $\mathcal{K} := k(e_1, \ldots, e_n)$ est le corps des coefficients de $pol(\boldsymbol{x})$
- corps des racines de $pol(\boldsymbol{x})$: $\mathcal{K}(\boldsymbol{x}) = k[\boldsymbol{x}]$
- $\mathrm{Gal}_{\mathcal{K}}(pol(\boldsymbol{x})) = \mathfrak{S}_n$ (penser correspondance galoisienne)
- $\mathcal{K}(\boldsymbol{x})^{\mathfrak{S}_n} = \mathcal{K}$; i.e. tout polynme symtrique s'exprime en les fonction symtriques lmentaires (thorme fondamental des fonctions symtriques)
- $L < \mathfrak{S}_n$, $\Theta \in k[\boldsymbol{x}]$; *rsolvante gnrique L-relative par* Θ
$$R_{\Theta,L} := \prod_{\Psi \in L.\Theta} (x - \Psi)$$
- $R_{\Theta,L}$ est le polynme minimal de Θ sur $\mathcal{K}(\boldsymbol{x})^L$
- $H < L < \mathfrak{S}_n$; Θ est un lment $\mathcal{K}(\boldsymbol{x})^L$-primitif du corps $\mathcal{K}(\boldsymbol{x})^H$ si et seulement si Θ est un H-invariant L-primitif (d'o la terminologie !)
- la H-rsolvante gnrique L-relative $R_{\Theta,L}$ d'un H-invariant L-primitif Θ :
$$R_{\Theta,L,\boldsymbol{x}} = \prod_{\tau \in L/H} (x - \tau.\Theta)$$
- le degr de l'extension $\mathcal{K}(\boldsymbol{x})^H$ du corps $\mathcal{K}(\boldsymbol{x})^L$ et l'indice de H dans L sont identiques :
$$[\mathcal{K}(\boldsymbol{x})^L : \mathcal{K}(\boldsymbol{x})^H] == [L : H]$$

- **Extension-contraction : corps et idaux galoisiens**
  (i) $\mathfrak{S}$ est le seul idal galoisien dfinit avec $\boldsymbol{x}$; i.e. tout sous-groupe de $\mathfrak{S}_n$ dfinit le mme idal galoisien, celui des relations symtriques entre les x_i.
  (ii) il existe une bijection entre les sous-groupes de $\mathfrak{S}_n$ et les corps intermdiaires entre k et $k(\boldsymbol{x})$

- lien avec l'idal des relations symtriques $\mathfrak{S}$:

$$R_{\Theta,\mathfrak{S}_n} == R_{\Theta,\mathfrak{S}}$$

- Attention : la notation $R_{\Theta,I} := R_{\Theta,L,\boldsymbol{\alpha}}$, I idal galoisien, n'est valide que pour $L = \mathrm{Max}(I, \boldsymbol{\alpha})$; donc ici, elle n'a de sens que pour $L = \mathfrak{S}_n$.

Evaluation : point de vue lagrangien

Posons $G = \mathrm{Gal}_k(\boldsymbol{\alpha})$.

- nous notons avec un $\tilde{}$ l'valuation envoyant x_i sur α_i

- $H < \mathfrak{S}_n$, $K := \mathcal{K}(\boldsymbol{x})^H$;

$$\widetilde{K} = k(\boldsymbol{\alpha})^{H\cap G}$$

- en particulier,
  (i) $(\forall H > G)$, $\widetilde{K} = k(\boldsymbol{\alpha})^G$
  (ii) $(\forall H < G)$, $\widetilde{K} = k(\boldsymbol{\alpha})^H$

- Evaluation de la rsolvante gnrique :

$$\widetilde{R_{\Theta,L}} = R_{\Theta,L,\boldsymbol{\alpha}}$$

- $H < L < \mathfrak{S}_n$, Θ H-invariant L-primitif, $\theta = \widetilde{\Theta}$; si θ est une racine simple de $R_{\Theta,L,\boldsymbol{\alpha}}$ alors θ est un lment $k(\boldsymbol{\alpha})^{L\cap G}$-primitif du corps $k(\boldsymbol{\alpha})^{H\cap G}$ de polynme minimal h sur $k(\boldsymbol{\alpha})^{L\cap G}$:

$$k(\boldsymbol{\alpha})^{H\cap G} = k(\boldsymbol{\alpha})^{L\cap G}(\theta)$$

  et, par consquent, $\deg_x(h) = [L \cap G : G \cap H]$

- C.P. si $G < L$ alors $k = k(\boldsymbol{\alpha})^{L\cap G}$, $R_{\Theta,L,\boldsymbol{\alpha}} \in k[\boldsymbol{x}]$ et

$$\deg_x(h) = [G : G \cap H]$$

- (effectivit du thorme de l'lment primitif) Soient $H_1 \subset H_2 \subset \mathrm{Gal}_k(\boldsymbol{\alpha})$, $K_i =: k(\boldsymbol{\alpha})^{H_i}$; Θ un H_1-invariant H_2-primitif $\boldsymbol{\alpha}$-sparable ; alors $\widetilde{\Theta}$ est un lment K_2-primitif de K_1 :
$$K_1 = K_2(\widetilde{\Theta})$$

- Soient G et H deux sous-groupes de S_n contenus dans L et tels que $L = GL = LH$ (si L est un groupe cela signifie que G et H sont deux sous-groupes de L) ; $L = \tau_1 H + \cdots + \tau_e H$; $H_i := H^{\tau_i}$; $\Theta_i := \tau_i \Theta$ est un H_i-invariant L-primitif ; $\theta_i := \widetilde{\Theta_i}$; soient $\theta_1, \ldots, \theta_r$ les s racines d'un facteur simple h de $R_{\Theta,L,\boldsymbol{\alpha}}$; o $V := \bigcap_{i=1}^{r} H_i$; alors
$$\mathrm{Gal}_k(h) = G/G \cap V;$$
pour $1 \leq i \leq r$, $\deg_x(h) = [G : G \cap H_i]$

- les groupes de Galois des facteurs d'une rsolvantes ainsi que leurs degrs respectifs sont obtenus par le thorme prcdent ; ils concident avec les matrices de groupes et de partitions de L (voir [19])

- Pour les cas des **racines non simples et des facteurs multiples de rsolvantes, les thormes se gnralisent** : voir [18] qui les illustre avec des exemples concrets.

References

[1] Ines Abdeljaouad. Calculs d'invariants primitifs de groupes finis. *Theor. Inform. Appl.*, 33(1):59–77, 1999.
(`http://www-gap.mcs.st-and.ac.uk/Gap3/Contrib3/contrib.html`).

[2] I. Abdeljaouad-Tej, S. Orange, G. Renault, and A. Valibouze. Computation of the decomposition group of a triangular ideal. *Appl. Algebra Engrg. Comm. Comput.*, 15(3-4):279–294, 2004.

[3] J.-M. Arnaudiès and A. Valibouze. Lagrange resolvents. *J. Pure Appl. Algebra*, 117/118:23–40, 1997.

[4] P. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. *J. Symbolic Comput.*, 30(6):635–651, 2000.

[5] Philippe Aubry and Annick Valibouze. Calcul algébrique efficace de résolvantes relatives. Archives HAL-CNRS, 07 2009.

[6] A. Cauchy. Usage des fonctions interpolaires dans la détermination des fonctions symétriques des racines d'une équation algébrique donnée. *Oeuvres*, **5**:473 Extrait 108, 1840.

[7] M. Lederer. Explicit constructions in splitting fields of polynomials. *Riv. Mat. Univ. Parma (7)*, 3*:233–244, 2004.

[8] Orange, S. and Renault, G. and Valibouze, A. Calcul efficace de corps de décomposition. Rapport 2003/005 du laboratoire LIP6 ; http://www.lip6.fr/, 2003. Dernires versions dans les thses de G. Renault (LIP6, 2005) puis S. Orange (LIP6, 2006).

[9] N. Rennert and A. Valibouze. Calculs de résolvantes avec les modules de Cauchy. *Experiment. Math.*, 8(4):351–366, 1999.
[10] J. McKay and R.-P. Stauduhar. Finding relations among the roots of an irreducible polynomial. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI)*, pages 75–77, New York, 1997. ACM.
[11] A. Valibouze. Étude des relations algébriques entre les racines d'un polynôme d'une variable. *Bull. Belg. Math. Soc. Simon Stevin*, 6(4):507–535, 1999. (Version longue du rapport LIP6 1997/014).
[12] A. Valibouze. Sur les relations entre les racines d'un polynme. *Acta Arithmetica*, 131.1:1–27, 2008.
[13] A. Valibouze. Dépendance algébrique des zéros de polynômes et groupes de Galois. *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)*, 48(96)(1):73–96, 2005.
[14] A. Valibouze. *Theory of Equations,Lagrange and Galois Theory*, 1995. Archives CEL-CNRS
[15] A. Valibouze. Base de Gröbner de l'idéal galoisien du groupe alterné. Archives HAL-CNRS, 02 2009.
[16] A. Valibouze. Idéaux galoisiens : Base de données. http://docs.google.com/Doc?id=dd9dj4wn_44hgttks3d Base de données d'idéaux galoisiens purs avec leur groupe de décomposition., 03 2009.
[17] A. Valibouze. La Résolvante de Lagrange et ses Applications. Archives HAL-CNRS, 04 2009.
[18] A. Valibouze. Résolvantes, groupe de Galois et Idéaux galoisiens. Archives HAL-CNRS, 10 2009.
[19] A. Valibouze. Computation of the Galois groups of the resolvent factors for the direct and inverse Galois problems. In *Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995)*, volume 948 of *Lecture Notes in Comput. Sci.*, pages 456–468. Springer, Berlin, 1995.
[20] A. Valibouze. Galois theory and reducible polynomials. Publication interne 99.03, quipe MAX, laboratoire LIX, cole Polytechnique, France, 1999. (`http://www.lix.polytechnique.fr/~max/publications/`).
[21] A. Valibouze. Classes doubles, idaux de Galois et rsolvantes. *Rev. R. de Math. Pures et Appl.*, 52 (2007), no 1, 95–109.
[22] K. Yokoyama. A modular method for computing the Galois groups of polynomials. *J. Pure Appl. Algebra*, 117/118:617–636, 1997. Algorithms for algebra (Eindhoven, 1996).
[23] K. Yokoyama. A modular method to compute the splitting field of a polynomial. *Communication prive*, 1999.

UPMC, 4, place Jussieu, 75252 Paris Cedex 05

E-mail address: `annick.valibouze@upmc.fr` `www-spiral.lip6.fr/~avb/`