Calcul de corps de décomposition
Utilisations fines d'ensemble de permutations en théorie de Galois effective

Soutenance de thèse de doctorat

Sébastien Orange

Université Pierre et Marie Curie

Laboratoire d'Informatique de Paris 6

Département Calcul scientifique

Équipe Systèmes Polynomiaux, Implantations, Résolution ALgébrique

.

Introduction

Que signifie résoudre l'équation polynomiale en une variable «$f = 0$» ?

Pouvoir calculer symboliquement les racines de f

Outil : Calcul formel pour représenter informatiquement le plus petit corps contenant les coefficients et les racines de f c'est à dire du

corps de décomposition de f

Sorties des algorithmes

- $\mathbb{K}$ un corps effectif
- $f \in \mathbb{K}[x]$ de degré n et $(\alpha_1, \ldots, \alpha_n)$ un n-uplet de ses racines
- $\mathbb{K}(\alpha_1, \ldots, \alpha_n)$: le corps de décomposition de f

$\Longrightarrow$ Représentation : $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{M}$
où $x_i \leftrightarrow \alpha_i$ et $\mathcal{M}$ est l'idéal engendré par toutes les relations algébriques en $x_1, \ldots, x_n$ satisfaites par $\alpha_1, \ldots, \alpha_n$

$\Longrightarrow$ L'action symbolique du groupe des automorphismes de $\mathbb{K}(\alpha_1, \ldots, \alpha_n)$ fixant $\mathbb{K}$ (le groupe de Galois de f)

Groupe de Galois $\leftrightarrow$ Corps de décomposition

Théorie de Galois effective

Contributions

Théoriques :

- idéaux de Galois
- lien entre groupes de Galois d'un polynôme et de ces facteurs irréductibles sur un corps de rupture

Algorithmiques :

- algorithmes de calcul du groupe de décomposition d'un idéal triangulaire
- algorithme mixte de calcul de corps de décomposition

Implantations (système de calcul formel `Magma`) :

- efficacités en temps de calcul

Représentations d'un corps de décomposition

- *Expression radicale des racines* : ([Abel, Galois...])
  $\rightarrow$ Impossible dans le cas général.

- *Élément primitif* ζ : $\mathbb{K}(\zeta) = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$
  Tout $\alpha \in \mathbb{K}(\alpha_1, \ldots, \alpha_n)$ s'écrit $P(\zeta)$.
  $\rightarrow$Représentation coûteuse (car deg(P) peut être égal à n!).

- *Idéal des relations* $\mathcal{M}$: $\mathbb{K}(\alpha_1, \ldots, \alpha_n) \simeq \mathbb{K}[x_1, \ldots, x_n]/\mathcal{M}$,
  où $\mathcal{M}$ est l'idéal maximal

$$\mathcal{M} = \{P \in \mathbb{K}[x_1, \ldots, x_n] \mid P(\alpha_1, \ldots, \alpha_n) = 0\}.$$

$\mathcal{M}$ dépend du n-uplet $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ des racines de f.
x_i : représentation symbolique de α_i.

Corps de décomposition et idéal des relations

- Base triangulaire de $\mathcal{M}$ (modules fondamentaux de Tchebotarev) :

$$\begin{cases} f_1(x_1) = x_1^{d_1} + g_1(x_1) \text{ avec } \deg_{x_1}(g_1) < d_1 \\ f_2(x_1, x_2) = x_2^{d_2} + g_2(x_1, x_2) \text{ avec } \deg_{x_2}(g_2) < d_2 \\ \quad \vdots \\ f_n(x_1, \ldots, x_n) = x_n^{d_n} + g_n(x_1, \ldots, x_n) \text{ avec } \deg_{x_n}(g_n) < d_n \end{cases}$$

Base de Gröbner

$\Downarrow$

Tests à 0 dans $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{M}$

$\Downarrow$

Calcul symbolique avec les racines de f

- Représentation $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha})$ du groupe de Galois de f = groupe de décomposition dans S_n de $\mathcal{M}$: $\{\sigma \in S_n \mid \sigma.\mathcal{M} = \mathcal{M}\}$

Corps de décomposition et idéal des relations

Exemple : $f(x) = x^4 - x^3 - 3x^2 + x + 1 \in \mathbb{Q}[x]$

- Pour un 4-uplet $\underline{\alpha} = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ de racines de f, une base triangulaire d'un idéal $\mathcal{M}$ des relations est :

$$\begin{cases} f_1(x_1) & = & x_1^4 - x_1^3 - 3x_1^2 + x_1 + 1, \\ f_2(x_1, x_2) & = & x_2 - x_1^3 + x_1^2 + 3x_1 - 1, \\ f_3(x_1, x_2, x_3) & = & x_3^2 + x_3 x_1^3 - x_3 x_1^2 - 2x_3 x_1 - 1, \\ f_4(x_1, x_2, x_3, x_4) & = & x_4 + x_3 + x_1^3 - x_1^2 - 2x_1. \end{cases}$$

- Formes normales $\Rightarrow$ identification dans $\mathbb{K}[x_1, x_2, x_3, x_4]/\mathcal{M}$
  Ex : $\alpha_1\alpha_2 = \alpha_3\alpha_4$ car $x_1x_2 - x_3x_4 = 0$ modulo $\mathcal{M}$
- Représentation du groupe de Galois correspondante :

$$\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha}) = \langle (1,2,3,4), (1,2)(3,4) \rangle$$

Plan

I Idéaux de Galois - Injecteurs

II Calcul du groupe de décomposition d'un idéal triangulaire

III Algorithme mixte de calcul d'un corps de décomposition

IV Idéaux de Galois d'un polynôme réductible

Idéaux de Galois et injecteurs

- f : polynôme en une variable à coefficients dans $\mathbb{K}$
- $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$: n-uplet des racines de f supposées distinctes

Idéal des relations : $\mathcal{M} = \{P \in \mathbb{K}[x_1, \ldots, x_n] \mid P(\underline{\alpha}) = 0\}$

Idéal des relations symétriques I_{Sym} : engendré par les modules de Cauchy de f

$$\begin{cases} f_1(x_1) = f(x_1) \\ \text{et, pour tout } i \in [\![2, n]\!], \\ f_i(x_1, \ldots, x_{i+1}) = \dfrac{f_{i-1}(x_1, \ldots, x_{i-2}, x_{i+1}) - f_{i-1}(x_1, \ldots, x_{i-1})}{x_{i+1} - x_{i-1}} \end{cases}$$

Idéaux de Galois et injecteurs

- f : polynôme en une variable à coefficients dans $\mathbb{K}$
- $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$: n-uplet des racines de f supposées distinctes

Idéal de Galois : idéal I tel que

$$\begin{array}{ccccc} I_{Sym} & \subseteq & I & \subseteq & \mathcal{M} \\ \downarrow & & \downarrow & & \downarrow \\ S_n.\underline{\alpha} & \supseteq & Inj(I,\mathcal{M}).\underline{\alpha} & \supseteq & \mathsf{Gal}_{\mathbb{K}}(\underline{\alpha}).\underline{\alpha} \end{array}$$

La partie $Inj(I, \mathcal{M})$ de S_n est l'injecteur de I relativement à $\underline{\alpha}$

$$Inj(I,\mathcal{M}) = \{\sigma \in S_n \mid \sigma.I \subset \mathcal{M}\}$$

II

Calcul du groupe de décomposition d'un idéal triangulaire

Algorithme **`Generators`** [Abdeljaouad, O., Renault, Valibouze 2004]
Algorithme **`EFG`** [O.2005]

Groupe de décomposition

Définitions

- Groupe de décomposition d'un idéal $I \subset \mathbb{K}[x_1, \ldots, x_n]$: stabilisateur dans S_n de I.

$$Dec(I) = \{\sigma \in S_n \mid \forall P \in I, \sigma.P \in I\}$$

- Un idéal de Galois dont tous les injecteurs coïncident avec $Dec(I)$ est dit pur.

Théorème [Aubry, Valibouze, 2000] :
Tout idéal de Galois pur est triangulaire

En particulier, nous avons $Dec(\mathcal{M}) = \mathrm{Gal}_{\mathbb{K}}(\underline{\alpha})$.

Groupe de décomposition

$[f_1(x_1), \ldots, f_n(x_1, \ldots, x_n)]$: base de Gröbner triangulaire de I
$Dec(I) = \{\sigma \in S_n \mid \forall i \in [\![1, n]\!],\ \sigma.f_i(x_1, \ldots, x_i) \in I\}$

Algorithme naïf

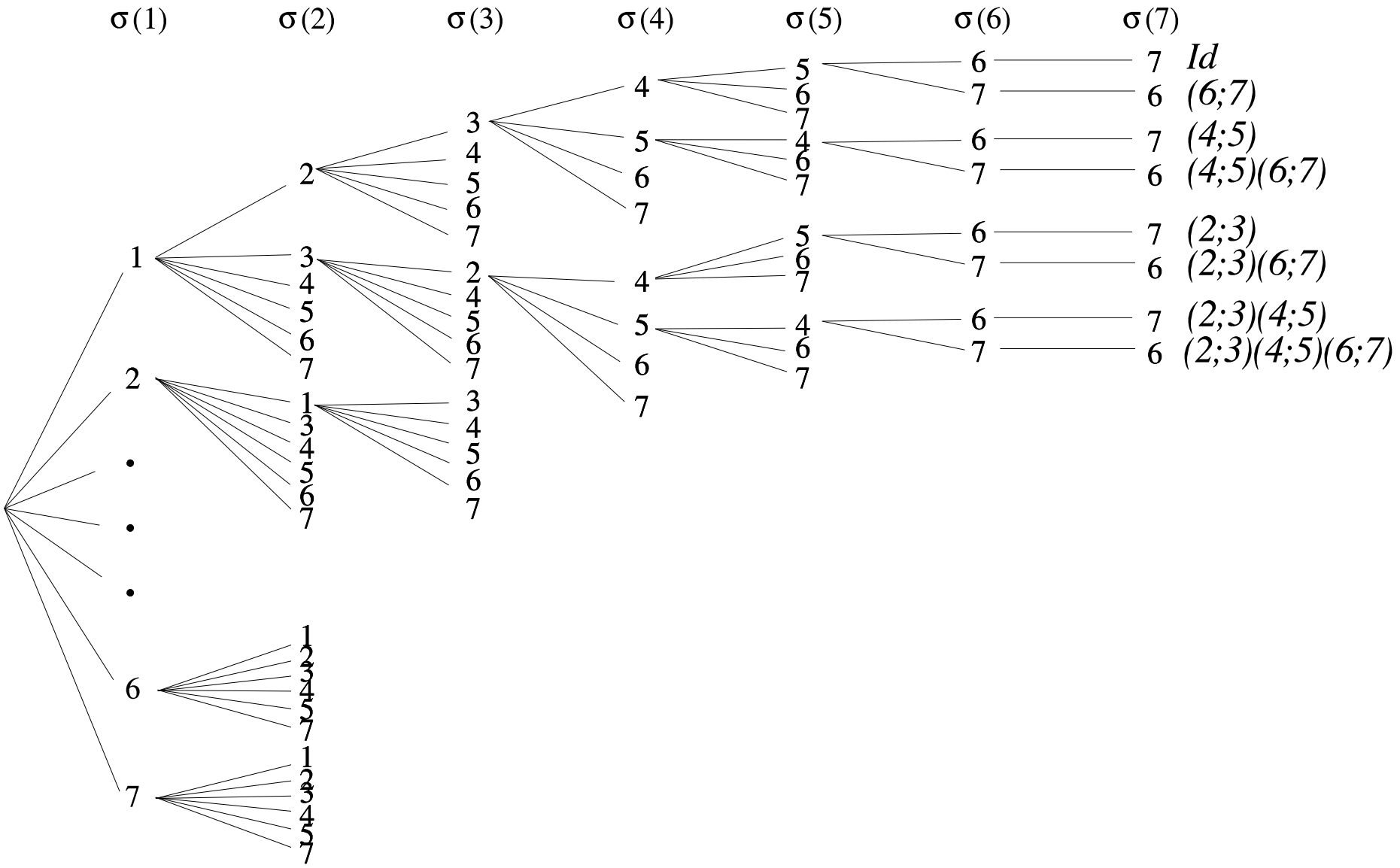
Entrée : $[f_1(x_1), \ldots, f_n(x_1, \ldots, x_n)]$
Sortie : toutes les permutations de $Dec(I)$

$\sigma \in Dec(I)$ ssi

$$\begin{cases} f_1(x_{\sigma(1)}) \in I, \\ \Rightarrow \text{ Recherche des } a_1 = \sigma(1) \text{ t q } f_1(x_{a_1}) \in I \\ f_2(x_{\sigma(1)}, x_{\sigma(2)}) \in I, \\ \Rightarrow \text{ Pour tout } a_1\text{, recherche des } a_2 = \sigma(2) \text{ t q } f_2(x_{a_1}, x_{a_2}) \in I \\ \vdots \\ f_n(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) \in I \\ \Rightarrow \text{ Tester si } f_n(x_{a_1}, \ldots, x_{a_{n-1}}, x_{a_n}) \in I \end{cases}$$

Groupe de décomposition

Un exemple de parcours d'arbre effectué par l'algorithme naïf



Groupe de décomposition

Stratégie de type *Branch and cut* [Sims, Butler, Leon...]

Notons $H_k = Fix_{Dec(I)}(\{1, \ldots, k\})$ $(= \{\sigma \in Dec(I) \mid \forall i \in [\![1, k]\!],\ \sigma(i) = i\})$

Algorithme **`Generators`** [Abdeljaouad, O., Renault, Valibouze 2004]

Entrée : $I = \langle f_1(x_1), \ldots, f_n(x_1, \ldots, x_n) \rangle$
Sortie : ensemble de générateurs de $Dec(I)$

Calculs : ensembles de générateurs des groupes

$$H_n \subseteq H_{n-1} \subseteq \cdots \subseteq H_2 \subseteq H_1 \subseteq Dec(I)$$

$$\langle H_k \cup \{\sigma_1, \sigma_2, \ldots\} \rangle = H_{k-1}$$

Les permutations σ_i vérifient

- $\sigma_i(1) = 1, \ldots, \sigma_i(k-1) = k-1$;
- $\sigma_i(k)$ élément minimal d'une H_k- orbite ;

et sont recherchées à l'aide l'algorithme naïf.

Groupe de décomposition

Stratégie de type *Branch and cut* [Sims, Butler, Leon...]

Notons $H_k = Fix_{Dec(I)}(\{1, \ldots, k\})$ $(= \{\sigma \in Dec(I) \mid \forall i \in [\![1, k]\!],\ \sigma(i) = i\})$

Algorithme **EFG** [O.2005]

Entrée : $I = \langle f_1(x_1), \ldots, f_n(x_1, \ldots, x_n) \rangle$
Sortie : ensemble de générateurs de $Dec(I)$

Calculs : ensembles de générateurs des groupes

$$H_n \subseteq H_{n-1} \subseteq \cdots \subseteq H_2 \subseteq H_1 \subseteq Dec(I)$$

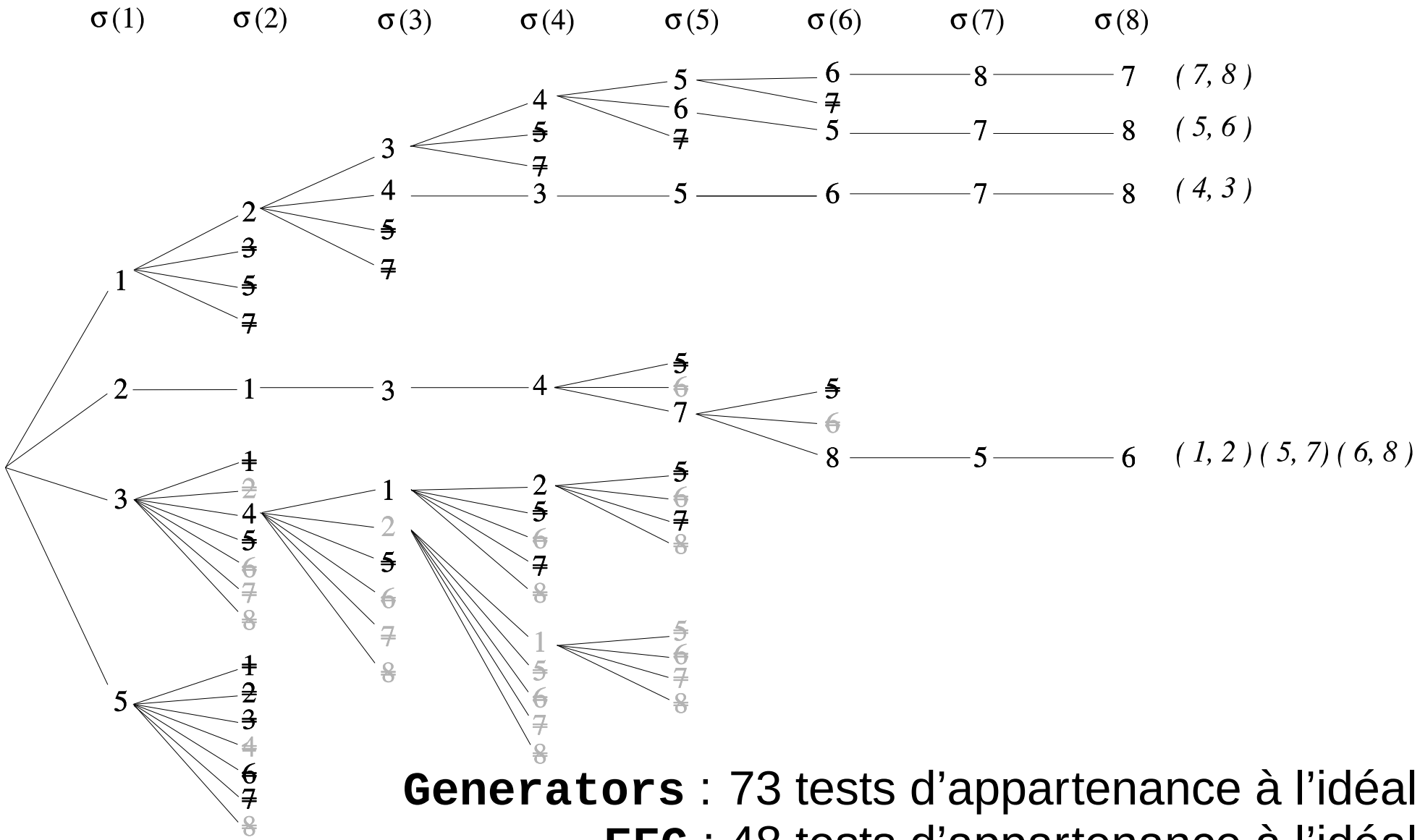
$$\langle H_k \cup \{\sigma_1, \sigma_2, \ldots\} \rangle = H_{k-1}$$

Les permutations σ_i vérifient

- $\sigma_i(1) = 1, \ldots, \sigma_i(k-1) = k-1$;
- $\forall r \in [\![k, n]\!],\ \sigma_i(r)$ élément minimal d'une $Fix_{H_k}(\{\sigma(1), \ldots, \sigma(r-1)\})$-orbite.

Groupe de décomposition

Exemples de parcours d'arbres effectués par les algorithmes



Generators : 73 tests d'appartenance à l'idéal

EFG : 48 tests d'appartenance à l'idéal

Complexité : nombre de tests d'appartenance

Algorithme **`StrongGenerators`** [Anai, Noro, Yokoyama 1996] :

- idéaux des relations : $O(n^4)$
- non applicable aux idéaux de Galois généraux

Algorithme **`Generators`** [Abdeljaouad, O., Renault, Valibouze 2004] :

- idéaux de Galois purs : au plus n^3
- pour certains idéaux de Galois : factoriel

Algorithme **`EFG`** [O.2005] :

- idéaux de Galois purs : au plus n^2
- idéaux de Galois : au plus $n^2 \frac{\#(L)^2}{\#(Dec(I)).\#(S)}$ où $S = \{\sigma \in S_n \mid \sigma.L \subset L\}$.

Comparaison des algorithmes : temps de calculs

Idéal	$Card(Dec(I))$	`StrongGenerators`	`Generators`	`EFG`
M_{8T10}	16	0.06	**0.02**	**0.02**
M_{8T17}	32	**0.24**	2.35	2.31
M_{8T26}	64	865.38	**2.04**	**2.04**
M_{8T35}	128	69.2	**0.15**	**0.16**
M_{9T28}	648	3.97	**0.19**	**0.2**
M_{10T43}	28 800	> 1000	0.74	**0.7**
M_{12T299}	1 036 800	> 1000	6.63	**6.14**
I_{12T26}	2304	-	4.2	**0.43**
I_{12T21}	480	-	78	**1.1**
I_{12T76}	28800	-	1	**0.3**
I_{12T183}	28800	-	49	**0.36**

Temps en secondes - Implantation en MAGMA

Athlon XP $2 \times$ 1,8 GHz - 1024 Mo

III

Un algorithme mixte de calcul de corps de décomposition

Algorithmes de calcul d'un idéal des relations

- f : polynôme irréductible de degré n

Construction théorique de Tchebotarev :

Factorisation de f sur $\mathbb{K}(\alpha_1)$, où α_1 racine de f

$$f(x) = (x - \alpha_1).f_2(\alpha_1, x)\ldots$$

Factorisation de f sur $\mathbb{K}(\alpha_1, \alpha_2)$, où α_2 racine de f_2

$$f(x) = (x - \alpha_1).(x - \alpha_2).f_3(\alpha_1, \alpha_2, x)\ldots$$

Factorisation de f sur $\mathbb{K}(\alpha_1, \alpha_2, \alpha_3)$, où α_3 racine de f_3

$\vdots$

Cette construction aboutit à un idéal des relations

$$\mathcal{M} = \langle f(x_1), f_2(x_1, x_2), f_3(x_1, x_2, x_3), \ldots, f_n(x_1, \ldots, x_n)\rangle$$

Algorithmes de calcul d'un idéal des relations

Implantation de la construction théorique de Tchebotarev ([Anai, Noro, Yokoyama], [Roblot]...)

Entrée : un polynôme f

Sortie : un idéal des relations de f

Calculs : factorisations dans des extensions algébriques

Coût croissant des factorisations

$\Downarrow$

Inefficacité des algorithmes

Algorithmes de calcul d'un idéal des relations

Algorithme GaloisIdéal [Valibouze, 97, 03]

Entrées : un idéal de Galois I_1 et un injecteur L_1 de I_1

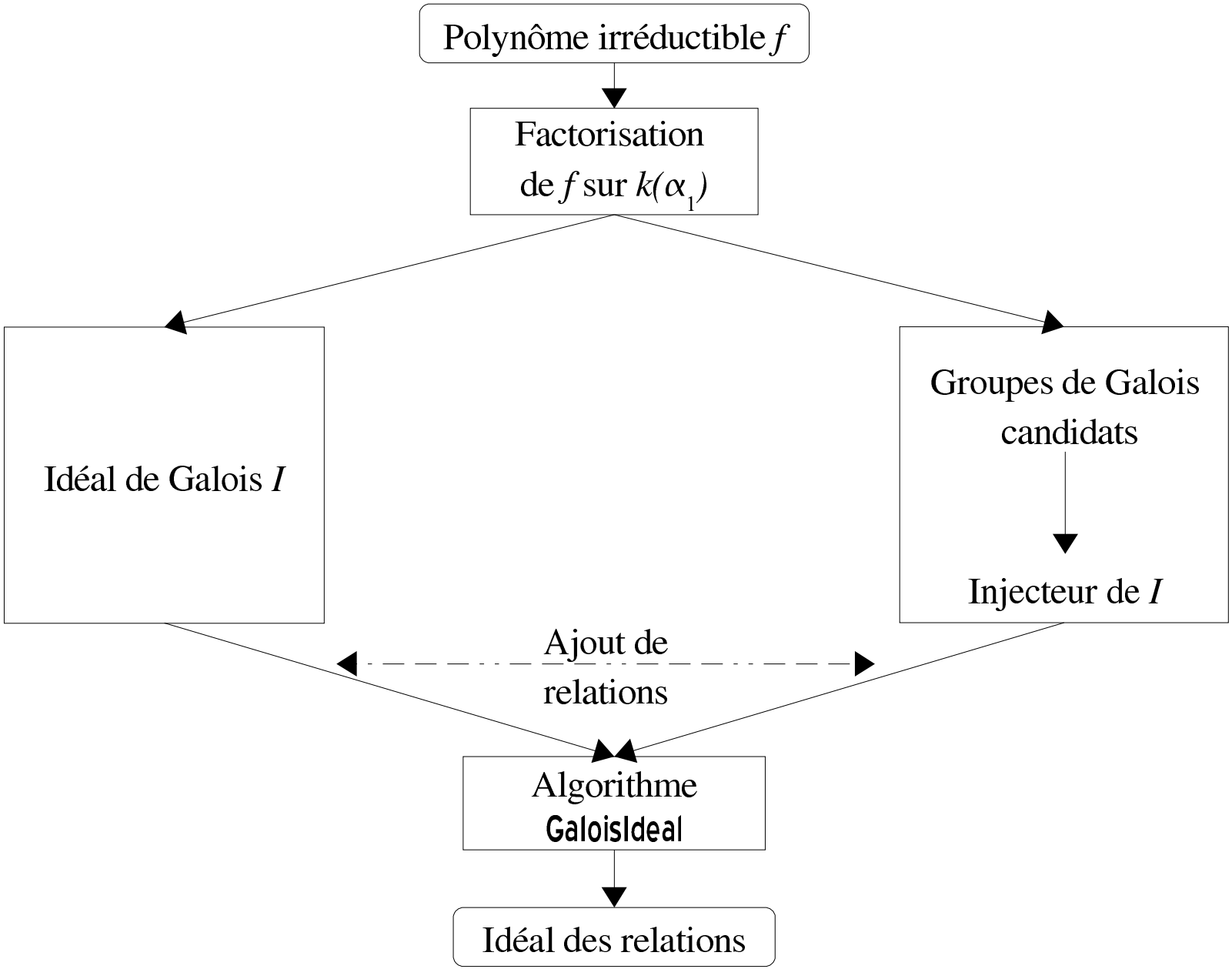
Sorties : un idéal des relations $\mathcal{M}$ et $Gal_{\mathbb{K}}(\underline{\alpha})$

Calculs :

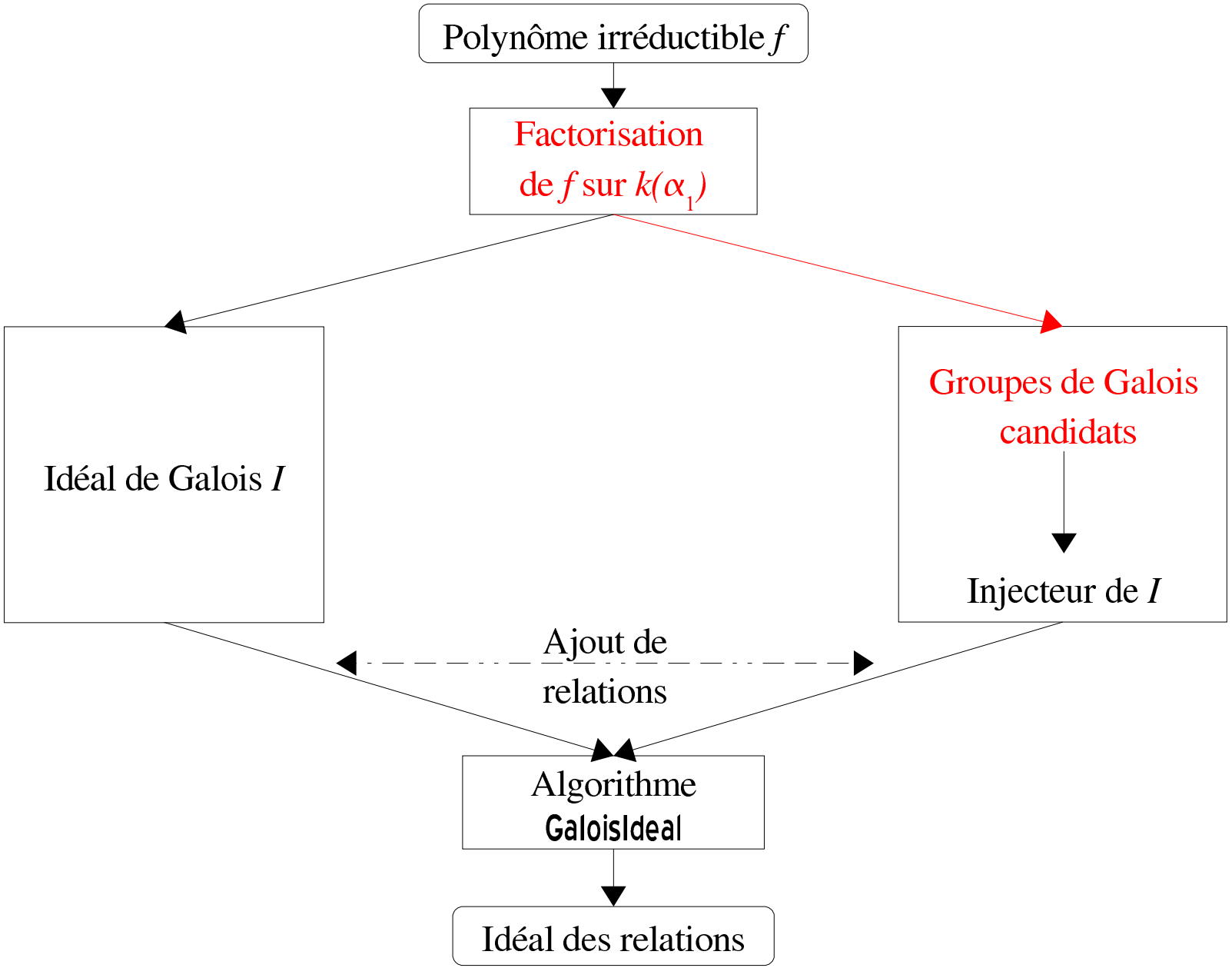
$$\begin{array}{ccccccc} I_1 & \subset & I_2 & \subset & \cdots & \subset & I_m = \mathcal{M} \\ L_1 & \supset & L_2 & \supset & \cdots & \supset & L_m = Gal_{\mathbb{K}}(\underline{\alpha}) \end{array}$$

$\langle I_k \cup R \rangle = I_{k+1}$ où R provient d'un calcul de résolvante.

Algorithme mixte



Algorithme mixte



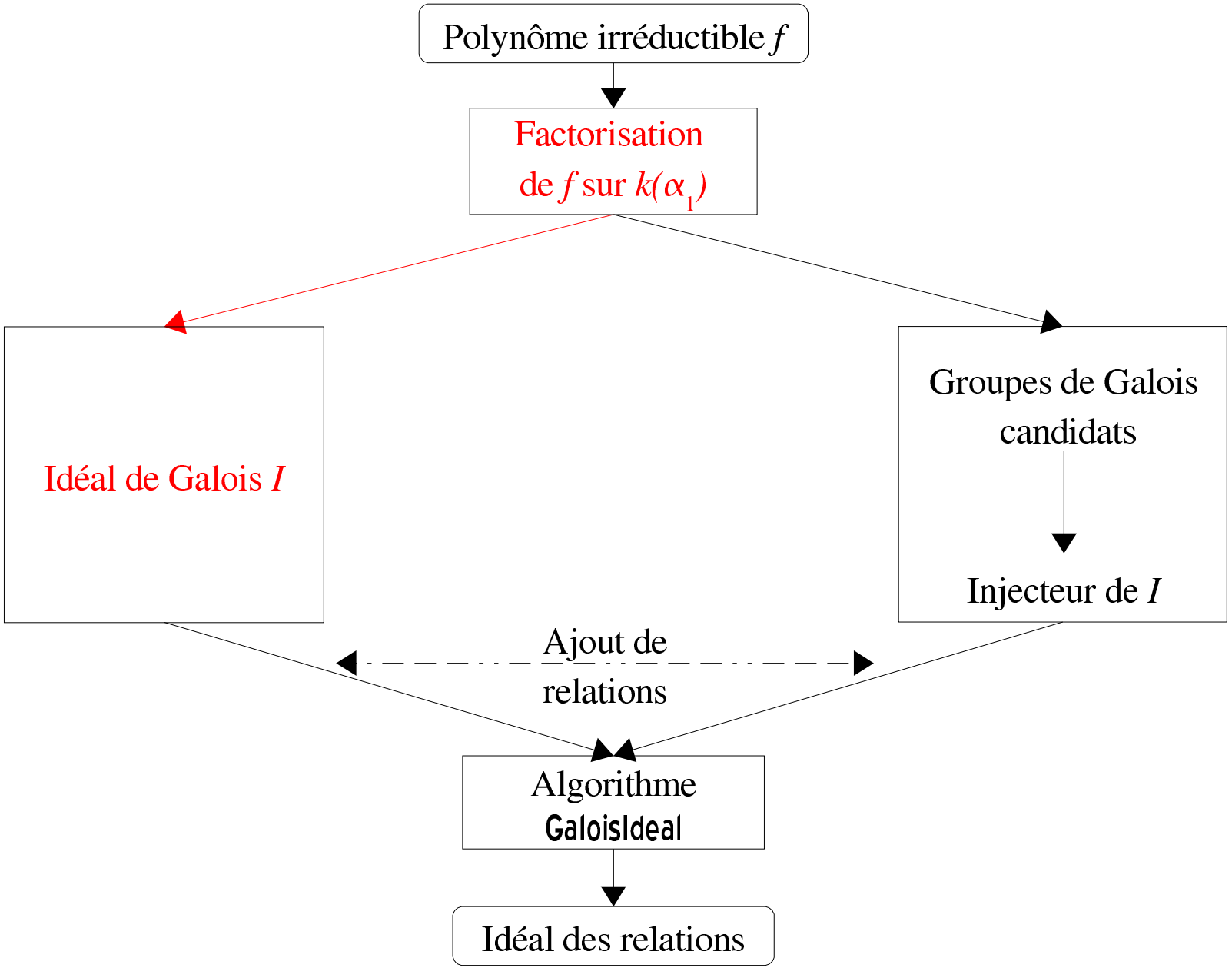
Factorisation et groupes de Galois

Tables de rupture [O., Renault, Valibouze, 2004]

Degrés des facteurs	Groupes de Galois des facteurs	$\mathrm{Gal}_{\mathbb{K}}(f)$	Cardinal
$[1^8]$	$(1T_1)^8$	$8T_1$	8
$[1^8]$	$(1T_1)^8$	$8T_2$	8
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_3$	$8T_{35}$	128
$[3^2,\ 1^2]$	$(1T_1)^2,\ (3T_1)^2$	$8T_{12}$	24
$[3^2,\ 1^2]$	$(1T_1)^2,\ (3T_1)^2$	$8T_{13}$	24
$[3^2,\ 1^2]$	$(1T_1)^2,\ (3T_1)^2$	$8T_{14}$	24
$[3^2,\ 1^2]$	$(1T_1)^2,\ (3T_2)^2$	$8T_{24}$	48
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_2$	$8T_{23}$	48
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_4$	$8T_{32}$	96
$\vdots$	$\vdots$	$\vdots$	$\vdots$

$\longrightarrow$ Discrimination différente de celle de [Soicher, McKay, 85]

Algorithme mixte



Algorithme mixte

Factorisation de f sur $\mathbb{K}[\alpha_1]$:

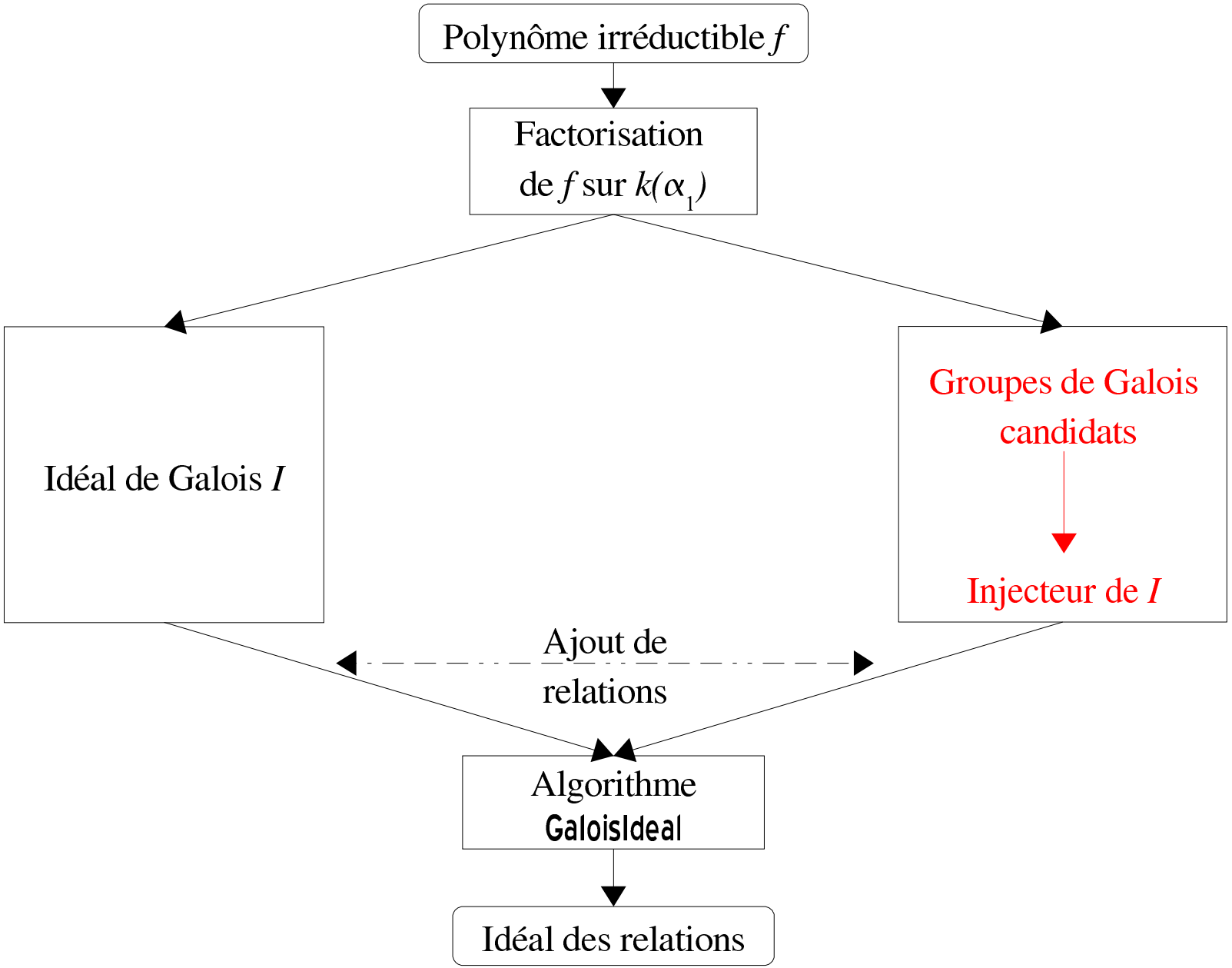
$$f(x) = (x - \alpha_1) g_2(\alpha_1, x) \dots g_r(\alpha_1, x)$$

Modules de Cauchy des facteurs $\Rightarrow$ ensemble triangulaire de polynômes :

$$\begin{cases} f(x_1) \\ g_2(x_1, x_2) = x_2^{d_2} + \cdots \\ \vdots \longleftarrow \textit{ Modules de Cauchy de } g_2 \\ \vdots \\ g_r(x_1, x_i) = x_i^{d_r} + \cdots \\ \vdots \longleftarrow \textit{ Modules de Cauchy de } g_r \end{cases}$$

Cet ensemble engendre un idéal de Galois I de f

Algorithme mixte



Algorithme mixte

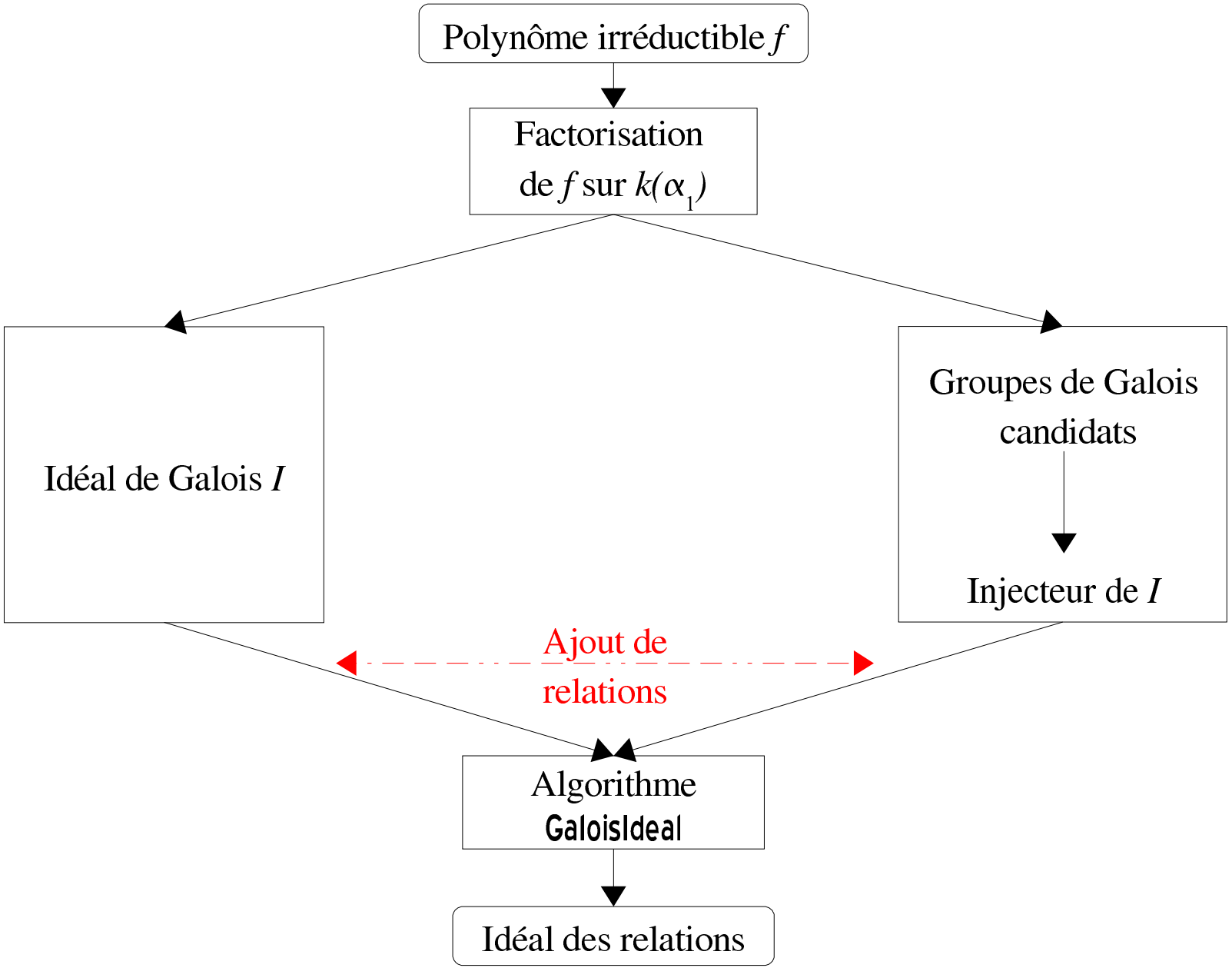
Comment déterminer un injecteur de l'idéal obtenu ?

- Caractérisation des parties d'un injecteur ([O.]).
  Notons $P.I = \{\sigma.g \mid \sigma \in P,\, g \in I\}$.

  Si P est une partie non vide d'un injecteur alors $\langle P.I \rangle \neq \mathbb{K}[x_1, \ldots, x_n]$.

- Critères peu coûteux :
  - propriété du groupe de Galois ;
  - calcul du groupe de décomposition (Algorithme EFG [O.]) ;
  - critères d'association.

Algorithme mixte



Algorithme mixte

Adjonction de relations par action de groupe.

Degrés des facteurs irréductibles de f sur $\mathbb{K}(\alpha_1)$: $[1, 1, 6]$.

$$\mathrm{Gal}_{\mathbb{K}}(f) \subset 8T_{44}$$

Modules de Cauchy des facteurs de $f \Rightarrow$ idéal de Galois :

$$\begin{cases} f_1(x_1) = x_1^8 + \cdots, \\ f_2(x_1, x_2) = x_2 + g_2(x_1) \\ f_3(x_1, x_3) = x_3^6 + \cdots \\ f_4(x_1, x_3, x_4) = x_4^5 + \cdots \\ f_5(x_1, x_3, x_4, x_5) = x_5^4 + \cdots \\ f_6(x_1, x_3, \ldots, x_5) = x_6^3 + \cdots \\ f_7(x_1, x_3, \ldots, x_7) = x_7^2 + \cdots \\ f_8(x_1, x_3, \ldots, x_8) = x_8 + \cdots \end{cases} \xrightarrow{\overrightarrow{\sigma_1, \sigma_2}} \begin{cases} f_1(x_1) = x_1^8 + \cdots, \\ f_2(x_1, x_2) = x_2 + g_2(x_1) \\ f_3(x_1, x_3) = x_3^6 + \cdots \\ \sigma_1.f_2 = x_4 + g_2(x_3) \\ f_5(x_1, x_3, x_4, x_5) = x_5^4 + \cdots \\ \sigma_2.f_2 = x_6 + g_2(x_5) \\ f_7(x_1, x_3, \ldots, x_7) = x_7^2 + \cdots \\ f_8(x_1, x_3, \ldots, x_8) = x_8 + \cdots \end{cases}$$

Injecteur de l'idéal de Galois obtenu : $8T_{44}$.

`GaloisIdeal` $\Rightarrow$ idéal des relations

Algorithme mixte

Adjonction de relations par action de groupe.

Degrés des facteurs irréductibles de f sur $\mathbb{K}(\alpha_1)$: $[1, 1, 6]$.

$$\mathrm{Gal}_{\mathbb{K}}(f) \subset 8T_{44}$$

Modules de Cauchy des facteurs de $f \Rightarrow$ idéal de Galois :

$$\begin{cases} f_1(x_1) = x_1^8 + \cdots, \\ f_2(x_1, x_2) = x_2 + g_2(x_1) \\ f_3(x_1, x_3) = x_3^6 + \cdots \\ f_4(x_1, x_3, x_4) = x_4^5 + \cdots \\ f_5(x_1, x_3, x_4, x_5) = x_5^4 + \cdots \\ f_6(x_1, x_3, \ldots, x_5) = x_6^3 + \cdots \\ f_7(x_1, x_3, \ldots, x_7) = x_7^2 + \cdots \\ f_8(x_1, x_3, \ldots, x_8) = x_8 + \cdots \end{cases} \xrightarrow{\overrightarrow{\sigma_1, \sigma_2}} \begin{cases} f_1(x_1) = x_1^8 + \cdots, \\ f_2(x_1, x_2) = x_2 + g_2(x_1) \\ f_3(x_1, x_3) = x_3^6 + \cdots \\ \sigma_1.f_2 = x_4 + g_2(x_3) \\ f_5(x_1, x_3, x_4, x_5) = x_5^4 + \cdots \\ \sigma_2.f_2 = x_6 + g_2(x_5) \\ f_7(x_1, x_3, \ldots, x_7) = x_7^2 + \cdots \\ f_8(x_1, x_3, \ldots, x_8) = x_8 + \cdots \end{cases}$$

$\rightarrow$ Gain : factorisations d'un polynôme de degré 5 sur une extension de degré 48 et d'un polynôme de degré 3 sur une extension de degré 192 !

Comparaison : temps de calculs

Gal(f)	|Gal(f)|	Fact. Ext.	Fact. Ext. et `GaloisIdeal`
$8T_{47}$	1152	**3732.05**	**0.21**
$8T_{46}$	576	**8400.61**	**519.29**
$8T_{45}$	576	**6040.89**	**179.55**
$8T_{44}$	384	**66.35**	**0.19**
$8T_{39}$	192	**10.54**	**0.17**
$8T_{35}$	128	**3.53**	**0.32**
$8T_{31}$	64	**0.66**	**0.26**
$8T_{29}$	64	**2.03**	**0.65**
$8T_{26}$	64	**1.8**	**1.44**
$8T_{19}$	32	**0.63**	**0.82**

Implantation en MAGMA

Temps en seconde - 2 $\times$ 933 Mhz - 1024 Mo

IV
Idéal de Galois d'un polynôme réductible
Application

Idéal de Galois d'un polynôme réductible

$f = g_1 g_2$: polynôme réductible séparable de degré n

Théorème[O., Renault, Valibouze 2005] : Si

- $I_1 = \langle \mathcal{G}_1 \rangle$: idéal de Galois de g_1 d'injecteur L_1 ;
- $I_2 = \langle \mathcal{G}_2 \rangle$: idéal de Galois de g_2 d'injecteur L_2 ;

alors $\langle \mathcal{G}_1 \cup \mathcal{G}_2 \rangle$ est un idéal de Galois de f d'injecteur $L_1 \times L_2$.

Application à l'algorithme mixte

Factorisation de f sur $\mathbb{K}(\alpha_1)$:

$$f(x) = (x - \alpha_1) g_2(\alpha_1, x).g_3(\alpha_1, x) \dots g_r(\alpha_1, x)$$

Idéaux de Galois des facteurs $g_2, g_3, \dots, g_r$

$\Downarrow$

Idéal de Galois de f

$\Downarrow$

Fin de l'algorithme mixte

$\Downarrow$

Idéal des relations

Conclusion - Perspectives

$\Rightarrow$ Algorithme efficace pour le calcul du groupe de décomposition

$\Rightarrow$ Algorithme mixte de calcul de corps de décomposition

$\Rightarrow$ Schéma de calcul pour utiliser les informations sur $\mathrm{Gal}_k(f)$ au fur et à mesure des factorisations

$\Rightarrow$ Amélioration de l'algorithme mixte

D'un idéal de Galois à un idéal de Galois pur

Proposition[O.] : Si I est un idéal de Galois dont un injecteur est L alors $id(L.I)$ est un idéal de Galois pur d'injecteur le groupe $S = \{\sigma \in S_n \mid \sigma.L \subset L\}$.

Ajout de relations dans l'algorithme mixte

$\Downarrow$

Idéal de Galois pur