Groupe de Galois et idéaux galoisiens : théorie, algorithmes et calculs

Séminaire Philosophie et Mathématiques

Annick Valibouze

Sorbonne Université

5 Mai 2025 ENS 45 Rue d'Ulm 75005 Paris

SCIENCES SORBONNE UNIVERSITÉ

Plan

- Partie 1 : Introduction - Historique
- Partie 2 : Théorie de Galois à la Galois et calcul du groupe de Galois
- Partie 3 : Idéaux galoisiens : groupe de Galois avec son action sur les racines et calculs dans le corps de racines

SCIENCES SORBONNE UNIVERSITÉ

Principaux Défis en Théorie de Galois

- **Détermination du groupe de Galois** d'un polynôme $p(x)$
- **Test à zéro** d'expressions polynomiales en les racines α_i de p

$$\alpha_1^2\alpha_3 - \alpha_2 + 7\alpha_4 = 0 \quad ?$$

- **Problème inverse de Galois** : *G groupe fini, groupe de Galois d'un polynôme ?* Exposé Pierre Dèbes Bicentenaire EG

http://www.galois.ihp.fr/wp-content/uploads/2012/03/P.-Debes.pdf

Pierre Cartier me montra que
le groupe à 168 éléments est
réalisé par le polynôme $p = x^7 - 7x + 3$.
Il utilisa la résolvante de p par $x_1 + x_2 + x_3$.

Dans les années 70, il calculait numériquement
des résolvantes avec Philippe Flajolet

SCIENCES SORBONNE UNIVERSITÉ

Les 3 grands problèmes grecs
Construire à la règle et au compas

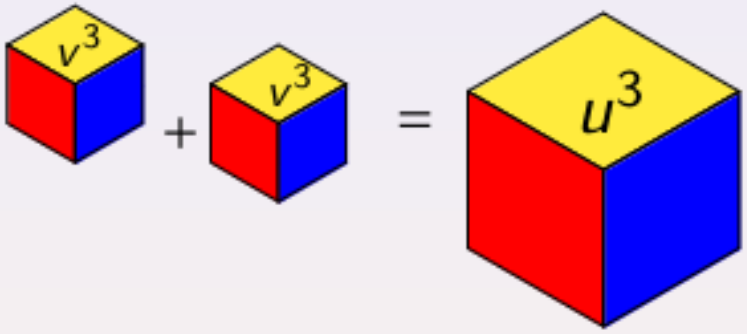
- Problème non algébrique

La quadrature du cercle : $a^2 = \pi r^2$

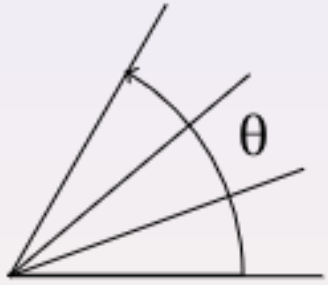
Ferdinand von Lindemann (1882) : transcendance de π

- Problèmes algébriques

Duplication du cube



Trisection de l'angle θ



$\theta = 60^o$
$x = cos(\theta/3)$

- Mise en équations avec Descartes (1596) :

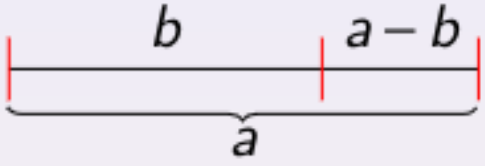
$x^3 - 2v^3 = 0$ $\qquad$ $8x^3 - 6x - 1 = 0$

- P.-L. Wantzel (1837) : *Construction R&C impossible si équation irréductible non puissance de 2*

Le nombre d'or

Un nombre, ancien de 10 000 ans, appelé aussi la divine proportion

- Architecture : temple d'Andros, pyramide de Khéops, Le "Modulor" de Le Corbusier,...
- Esthétique et art : Dali, Picasso, statue d'Athéna Parthénos, ...
- Phyllotaxie (*disposition des feuilles autour de la tige des plantes*)



$$\varphi = \frac{a}{b} = \frac{b}{a-b}$$

$$\varphi^2 - \varphi - 1 = 0$$

Le nombre d'or φ est la solution positive de l'équation

$$x^2 - x - 1 = 0$$

Des deux valeurs suivantes, laquelle préférer ?

$$\varphi = \frac{1+\sqrt{5}}{2} \simeq 1.6180339887$$

Numérique ou Algébrique ? avec Maxima

In [7]: `p:x^2-x-1$` polynôme $p = x^2 - x - 1$

In [8]: `solve(p);` Solutions algébriques ?

Out[8]: `[x=(1 + sqrt(5))/2,x=(1- sqrt(5))/2]`

In [9]: `sol_alg:(1+sqrt(5))/2$` $= \varphi = \frac{1+\sqrt{5}}{2}$

In [10]: `sol_numer: float(sol_alg);`

Out[10]: `1.618033988749895` approximation numérique $\widetilde{\varphi}$ de φ

In [11]: `subst(sol_alg,x,p);` $p(\varphi) = ?$

Out[11]: `0` $p(\varphi) = 0$

In [12]: `subst(sol_numer,x,p);` $p(\widetilde{\varphi}) = ?$

Out[12]: `0.0` Résultat assez proche de 0 : $p(\widetilde{\varphi}) \simeq 0$

In [13]: `subst(1.61803398874989,x,p);`

Dernier chiffre significatif oté à sol_numer

Out[23]: `-1.065814103640150 3e-14`

Résultat ''considéré'' comme non nul

SCIENCES SORBONNE UNIVERSITÉ

Nombres algébriques et Polynômes

Polynômes $3x^3-2, \quad x^2-x-1, \quad x^6-1$

$$p = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \quad a_i \in \mathbb{Z},\ n \in \mathbb{N},\ a_n \neq 0$$

Racines d'un polynôme : valeurs qui l'annulent : 3 annule $x-3$

Nombre de racines = puissance maximale n = degré de p

p s'exprime en fonction de ses n racines $\alpha_1, \alpha_2, \ldots, \alpha_n$

$$p = a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \quad \text{(D'Alembert-Gauss)}$$

Nombres Rationnels : $\frac{a}{b}$ racine du polynôme $bx-a$

Dupliquer le cube de coté v : u racine (réelle) de x^3-2v^3

Trisection de l'angle : $\cos(20°)$ racine de $8x^3-6x-1$

Nombre d'or φ : $x^2-x-1=(x-\varphi)(x-\frac{1-\sqrt{5}}{2})$

Nombre π n'est pas algébrique, il est transcendant.

SCIENCES SORBONNE UNIVERSITÉ

La théorie algébrique des équations

Étude et "calculs" algébriques des solutions des équations

Objectif : Réaliser des calculs exacts avec les racines de polynômes

Première approche : La résolution par radicaux

Exprimer les racines en termes d'opérations élémentaires et de radicaux dépendant des coefficients

Figure: Joseph-Louis Lagrange 1736-1813

SCIENCES SORBONNE UNIVERSITÉ

Résolution par radicaux

Degré 2

$$x^2 + bx + c = (x - \frac{-b - \sqrt{b^2 - 4c}}{2})(x - \frac{-b + \sqrt{b^2 - 4c}}{2})$$

Deg. 3,4 Formules Del Ferro, Tartaglia, Ferrari, Cardan XVI-ème
Algorithmes : Vandermonde, Lagrange XVIII-ème

```
In [27]: solve(x^3-7*x+11);
Out[27]:
x= (√1895/(2*3^(3/2))-11/2)^(1/3)
                    +7/(3*(√1895/(2*3^(3/2))-11/2)^(1/3))
x=7*(√3*%i/2-1/2)/(3*(√1895/(2*3^(3/2))-11/2)^(1/3))
    +(√1895/(2*3^(3/2))-11/2)^(1/3)*(-√3*%i/2-1/2)
x= (√1895/(2*3^(3/2))-11/2)^(1/3)*(√3*%i/2-1/2)

    +7*(-√3*%i/2-1/2)/(3*(√1895(2*3^(3/2))-11/2)^(1/3))
```

⇒ S'affranchir de la résolution par radicaux ?
... comme de la règle et du compas

SCIENCES SORBONNE UNIVERSITÉ

Résolvante de Lagrange et Résolution

Idée Equation de degré 4 $\Rightarrow$ degré 3 $\Rightarrow$ degré 2

Outil Résolvante R de p par un invariant $f(x_1,\ldots,x_n)$:

1- Permuter f : prenons $f = x_1x_2 + x_3x_4$ et degré$(p) = 4$

24 permutations mais seulement 3 permutés distincts de f :

f, $\quad x_1x_3 + x_2x_4 = (2,3)\cdot f$, $\quad x_1x_4 + x_2x_3 = (2,4)\cdot f$

2- Racines de R = évalués de ces permutés en les racines de p

Algorithme Théorème fondamental des fonctions symétriques effectif

Résolvante diédrale : $p = x^4 - 8x^3 + 5x + 1$ par $f = x_1x_2 + x_3x_4$

```
In [28]: resolvante_diedrale(x^4-8*x^3+5*x+1,x);
Out[28]: x^3 - 44x - 89
```

Conjecture Lagrange (1770) Pas toujours possible au delà du degré 4

Théorème Abel (1824) Polynôme de degré 5 non résoluble par radicaux

Théorème Galois ($\approx$ 1831) Critère alg. pour la résolution par radicaux

SCIENCES SORBONNE UNIVERSITÉ

Résolution et Informatique $\deg(p) = n$

Calculs	(XVI-ième au XVIII-ième S.) résolution par radicaux pour $n \leq 4$
Idée	Lagrange (1770) Rabaisser le degré n en transformant par
Outil	des Résolvantes (absolues) $\Rightarrow$ calculs
Idée	Galois (1831) Gal(p), groupe de Galois de $p \Rightarrow$ calculs
Théorie	p résoluble par radicaux ssi Gal(p) résoluble $\Rightarrow$ calculs
Théorème	Cayley (1861) Sa résolvante teste la résolution en degré $n = 5$
Idées	Artin (1944) Extensions galoisiennes, automorphismes ...
Théorie	abstraite $\Rightarrow$ Correspondance galoisienne
Calculs	Stauduhar (1973) Gal(p) : algébro-numérique + graphe inclusion
Calculs	Dummit (1991) Équations résolubles en degré $n = 5$
Théorie	Berwick ($n = 6$, 1929), McKay-Soicher ($n \leq 11$, 1983), Arnaudiès-AV. ($\forall n$, 1993), AV ($\forall n$, 1995) Gal(p) avec des résolvantes et matrices de partitions ou de groupes $\Rightarrow$ calculs
Calculs	Hagedorn (2000) Équations résolubles en degré $n = 6$

SCIENCES SORBONNE UNIVERSITÉ

Partie 2

Théorie de Galois à la Galois et calcul du groupe de Galois

Résolvantes, invariants primitifs, matrice des partitions,

SCIENCES SORBONNE UNIVERSITÉ

Théorie de Galois à la Galois

(*présentation à prendre avec des pincettes : voir la suite*)

- $p = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \quad a_i \in \mathbb{Z},\ n \in \mathbb{N}, a_n \neq 0$
  Racines inconnues (a priori) et 2 à 2 distinctes : $\alpha_1, \ldots, \alpha_n$

Définition de la Résolvante de Galois

Polynôme R dont les racines sont les $n! = n(n-1)(n-2)\cdots 1$ "permutés" "distincts" de $v = \alpha_1 + 2\alpha_2 + 3\alpha_3 + \cdots + n\alpha_n$

- $V = x_1 + \cdots + n x_n$: $(1,2) \cdot V(\boldsymbol{\alpha}) = \alpha_2 + 2\alpha_1 + 3\alpha_3 + \quad + n\alpha_n$
- R se factorise sur $\mathbb{Q}$ en $\frac{n!}{e}$ polynômes irr. de même degré e.

Définition du Groupe de Galois $\mathrm{Gal}(p)$ de p sur $\mathbb{Q}$

Ensemble des e permutations qui envoient v sur $v = v_1, \ldots, v_e$, les racines d'un même facteur irréductible sur $\mathbb{Q}$ de R .

Théorème Fondamental de Galois

Toute expression polynomiale en les racines de p invariante par $\mathrm{Gal}(p)$ est rationnelle et réciproquement.

SCIENCES SORBONNE UNIVERSITÉ

Intérêt du groupe de Galois pour le Calcul

Polynômes de degré n : une infinité
Groupes de permutations de degré n : un nombre fini

Le groupe de Galois fournit des informations capitales pour

- Résoudre p par radicaux : ssi Gal(p) est résoluble (Galois)
- Obtenir les idéaux galoisiens afin de réaliser des calculs exacts avec les racines : test à zéro, résolvantes relatives, etc ...
- Mesurer l'indétermination entre les racines
  - $p = (x-1)(x-2) = x^2 - 3x + 2$
    Gal(p)$= Id = \{(1)(2)\}$ 1 élément ; racines discernables
  - $p = x^3 - 6$ et $V = x_1 + 2x_2 + 3x_3$
    Factorisation de sa résolvante de Galois de degré 3!=6 :

    In [7]: factor(resolvante(x^3-6,x,x1+2*x2+3*x3,[x1,x2,x3]));
    Out[7]: $y^6 + 972$

    Gal(p) 6 éléments selon Galois $\Rightarrow$ racines indiscernables

SCIENCES SORBONNE UNIVERSITÉ

Pourquoi l'informatique pour les groupes ?

Cole en 1893 complète la liste établie en 1891 pour $n \leq 8$

1893

NOTE ON THE SUBSTITUTION GROUPS OF SIX, SEVEN, AND EIGHT LETTERS.

BY F. N. COLE, PH.D.

A LIST of the groups of six, seven, and eight letters is given by Mr. Askwith in vol. 24 of the *Quarterly Journal of Mathematics*, and Professor Cayley has revised and tabulated Mr. Askwith's results in vol. 25 of the same journal.* Noticing that several familiar groups were missing in this table, I have re-examined the whole question by an independent method, with the result that I am able to furnish here a supplementary list of over forty omitted groups of these degrees. The precautions which I have taken to insure accuracy give me a considerable degree of confidence that my results are correct and complete.

I. *Six and Seven Letters.*

1. For six letters the intransitive and multiply transitive groups are correctly given in Professor Cayley's enumeration. The three following non-primitive groups are, however, omitted:

Order 36. $36_9 =$

+	+	+	+	−	−
1,	*abc*,	*abc . def*,	*ab . de*,	*ad . be . cf*,	*adbecf*,
	acb,	*abc . dfe*,	*ab . df*,	*ad . bf . ce*,	*adbfce*,
	def,	*acb . def*,	*ab . ef*,	*ae . bd . cf*,	*adcebf*,
	dfe,	*acb . dfe*,	*ac . de*,	*ae . bf . cd*,	*adcfbe*,
			ac . df,	*af . bd . ce*,	*aebdcf*,
			ac . ef,	*af . be . cd*,	*aebfcd*,
			ad . be,	*ab . cd . ef*,	*afbecd*,
			ad . bf,	*ac . bd . ef*,	*afcebd*,
			ad . ef,	*ae . bd . cf*,	*afcdbe*,
			ae . bd,	*ae . bf . cd*,	*afdbce*,
			ae . bf,	*af . bd . ce*,	*afdcbe*,
			ae . cf,	*af . be . cd*,	*afebcd*,
			af . bd,	*ab . cd . ef*,	*afecbd*,
			af . be,	*ac . bd . ef*,	*afedbc*,
			af . ce,	*ad . be . cf*,	
			af . cd,	*ad . bf . ce*,	

GAP (donc SageMaths) - A. Hulpke (1990)

Calculs et tabulation des générateurs jusqu'au degré 30.

Classes de conjugaison en degré 4 :

```
gap> S4:=SymmetricGroup(4);;
gap> ConjugacyClassesSubgroups(S4);;
```

	Nature	Ordres
H_1	S_4	24
H_2	A_4	12
H_3	D_4	8
H_4	$Id \times S_3$	6
H_5	C_4	4
H_6	V_4	4
H_7	$S_2 \times S_2$	4
H_8	$A_3 \times S_1$	3
H_9	$<(1,2)(3,4)>$	2
H_{10}	$S_1 \times S_1 \times S_2$	2
H_{11}	I_4	1

Intérêt des invariants (primitifs)

La résolvante $R(p, f)$ résulte d'une certaine transformation de $p(x)$ de groupe de Galois G par $f(x_1, \ldots, x_n)$, polynôme sur $\mathbb{Q}$.

- Résolution par radicaux
- Détermination du groupe de Galois
- Calcul des relations entre les racines (idéaux galoisiens)

Définition. $f(x_1, \ldots, x_n)$ est un H-*invariant primitif* s'il identifie le groupe H dans S_n : H=Stab$_{S_n}(f)$

Le groupe H est un **testeur** dans S_n des groupes à être le groupe de Galois G et plus encore ... avec des calculs sur $\mathbb{Q}$ via la résolvante $R(p, f) \in \mathbb{Q}[x]$.

$$\text{Indice de } H \text{ dans } S_n = \text{degré } R(p, f).$$

(*Plus loin : tout sous-groupe L de S_n peut remplacer S_n si $G < L$*)

SCIENCES SORBONNE UNIVERSITÉ

Invariants des groupes en degré 4

Ex. $f = Va = \prod_{i<j}(x_i - x_j)$, le Vandermonde, un invariant primitif de $H{=}A_4$ d'indice 2 dans S_4 et on a $S_4 \star Va = \{Va, -Va\}$.
Posons $\widetilde{Va} = Va(\alpha_1, \ldots, \alpha_4)$. Si p unitaire alors $Disc(p) = \widetilde{Va}^2$ et

$$R(p, f) = (x - \widetilde{Va})(x + \widetilde{Va}) = x^2 - Disc(p) \in \mathbb{Q}[x]$$

Noms	Indices	Invariants primitifs
$H_1 = S_4$	1	1 ou tout polynôme symétrique en $x_1, \ldots, x_4$
$H_2 = A_4$	2	Va
$H_3 = D_4$	3	$x_1x_2 + x_3x_4$
H_4	4	x_1
$H_5 = C_4$	6	$(x_1 - x_2)(x_2 - x_3)(x_3 - x_4)(x_4 - x_1)$
$H_6 = V_4$	6	$(x_1 - x_2)(x_3 - x_4)$
H_7	6	$x_1 + x_2$
H_8	8	$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$
H_9	12	$x_1x_3^2 + x_2x_4^2$
H_{10}	12	$x_1 - x_2$
$H_{11} = I_4$	24	$x_1 + 2x_2 + 3x_3$ ou $x_1x_2^2x_3^3$

SCIENCES SORBONNE UNIVERSITÉ

Calculs d' invariants

Foulkes, 1930, *The resolvents of an equation of the seventh degree*

(*b*) **The function***

$$\psi_0 = \gamma\alpha\delta+\delta\beta\epsilon+\epsilon\gamma\zeta+\zeta\delta\eta+\eta\epsilon\alpha+\alpha\zeta\beta+\beta\eta\gamma$$

is unaltered by U and W and takes up thirty different forms when operated on by all the substitutions of the symmetric group. The function belongs therefore to Γ_{168}, whose index is 30. Every function belonging to Γ_{168} possesses the property, observed by Noether,† of being expressible in seven 'triplets'. Kronecker,‡ in 1858, gave

$$(\gamma+\alpha+\delta)(\delta+\beta+\epsilon)(\epsilon+\gamma+\zeta)(\zeta+\delta+\eta)(\eta+\epsilon+\alpha)(\alpha+\zeta+\beta)(\beta+\eta+\gamma)$$

C'est la résolvante absolue R de degré 35 par l'invariant $x_1+x_2+x_3$ que cherchaient à calculer Pierre Cartier et Philippe Flajolet avec de l'algébro-numérique, comme le proposait en 1973 Richard Stauduhar, lui pour calculer les résolvantes dites relatives ; i.e. sans le théorème fondamental des fonctions symétriques. Le groupe de Galois de x^7-7x+3 est le sous-groupe transitif de S_7 d'ordre 168 ssi R se factorise en deux polynômes, l'un de degré 7 et l'autre de degré 28.

SCIENCES SORBONNE UNIVERSITÉ

Sous le logiciel GAP

- Algorithme : Girstmair, 1987
- Algorithme et Implantation : I. Abdeljaouad, 1998, Package GAP

Un H-invariant S_8-primitif en degré 8 avec GAP

```
gap>Read("PrimitiveInvariant.g");
gap> s8:=SymmetricGroup(8);
gap> H:=Subgroup(s8,[(1, 4)(2, 3)(5, 8)(6, 7), (1, 2)(3, 4)(5, 6)(7,
8), (1, 5)(2, 6)(3, 7)(4, 8), (1, 2)(5, 7, 6, 8)]);;
gap> MinimalPrimitiveInvariants(8,s8,H);
x4*x6*x8^2+x4*x7*x6^2+x4*x8*x5^2+x4*x5*x7^2+x3*x6*x8^2
+x3*x7*x6^2+x3*x8*x5^2+x3*x5*x7^2+x2*x8*x6^2+x2*x6*x7^2
+x2*x5*x8^2+x2*x7*x5^2+x2*x8*x4^2+x2*x7*x4^2+x4*x6*x2^2
+x4*x5*x2^2+x3*x8*x2^2+x3*x7*x2^2+x2*x6*x3^2+x2*x5*x3^2
+x1*x8*x6^2+x1*x6*x7^2+x1*x5*x8^2+x1*x7*x5^2+x4*x8*x1^2
+x4*x7*x1^2+x1*x6*x4^2+x1*x5*x4^2+x1*x8*x3^2+x1*x7*x3^2
+x3*x6*x1^2+x3*x5*x1^2
```

Comment calculer un groupe de Galois ?

Protagonistes :
- $p(x)$ notre polynôme de degré n
- H et H' deux groupes (connus sous GAP => sous SageMath)

Outils programmables :
- Une certaine partition d'entiers $[H, H']$ pré-calculée (GAP)
- $f(x_1, \ldots, x_n)$ un H-invariant S_n-primitif (GAP)
- Résolvante (absolue) R de p par f (Maxima => SageMath)

Théorème (Arnaudiès-V., 1993)

Si R sans racine double (toujours possible)
1- $H' = \mathrm{Gal}(p) \Rightarrow [H, H'] =$ *degrés des facteurs de* R
2- $\mathrm{Gal}(p)$ *est déterminable ainsi en tout degré* n

Note : Remplacer $[H, H']$ par une certaine liste de groupes => gains importants et polynômes de groupe de Galois donné (AV, 1995)

SCIENCES SORBONNE UNIVERSITÉ

Matrice des partitions (absolue) en degré 4

Première Colonne : groupes Tests
Première Ligne : groupes Candidats à être le groupe de Galois
Ligne H_i - Colonne $H_j = [H_i, H_j]$
cardinaux des H_j-orbites des classes à gauche de $S_n \bmod H_i$

Test H_5 : $R(p,f) = (x^2 + \cdots)(x^4 + \cdots) \Rightarrow \mathrm{Gal}(p) \in \{H_3\ ,\ H_7\}$
Test H_4 : $R(p,x_1) = p = x^4 + \cdots$ irréductible$\Rightarrow \mathrm{Gal}(p) = H_3 = D_4$

	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8	H_9	H_{10}
H_2	2	1^2	2	2	2	1^2	2	1^2	1^2	2
H_3	3	3	1,2	3	1,2	1^3	1,2	3	1^3	1,2
H_4	4	4	4	1,3	4	4	2^2	1,3	2^2	1^2,2
H_5	6	6	2,4	6	1^2,4	2^3	2,4	3^2	1^2,2^2	2^3
H_6	6	3^2	2^3	6	2^3	1^6	2^3	3^2	1^6	2^3
H_7	6	6	2,4	3^2	2,4	2^3	1^2,4	3^2	1^2,2^2	1^2,2^2
H_8	8	4^2	8	2,6	4^2	4^2	4^2	1^2,3^2	2^4	2^4
H_9	12	6^2	4^3	6^2	2^2,4^2	2^6	2^2,4^2	3^4	1^4,2^4	2^6
H_{10}	12	12	4,8	3^2,6	4^3	4^3	2^2,4^2	3^4	2^6	1^2,2^5
H_{11}	24	12^2	8^3	6^4	4^6	4^6	4^6	3^8	2^{12}	2^{12}

SCIENCES SORBONNE UNIVERSITÉ

Un exemple

In 2 $p : x^4 + 8 * x + 12\$$

In 3 factor(p4); testeur $= H_4$ et invariant $f = x_1$

Out 3 $X^4 + 8X + 12 \Rightarrow [H_4, \mathrm{Gal}(p)] = 4$

	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8	H_9	H_{10}
H_4	4	4	4	1,3	4	4	2^2	1,3	2^2	1^2,2

In 4 factor(poly_discriminant(p,x)); $R(p, Va) = x^2 - \mathrm{Disc}(p)$

Out 4 $2^{12}3^4 \Rightarrow [H_2, \mathrm{Gal}(p)] = 1^2$

	H_1	H_2	H_3	H_5	H_6
H_2	2	1^2	2	2	1^2

In 5 factor(resolvante_diedrale(p,x)); $f = x_1x_2 + x_3x_4$

Out 5 $X^3 - 48X - 64 \Rightarrow [H_3, \mathrm{Gal}(p)] = 3$

	H_2	H_6
H_3	3	1^3

$\Rightarrow$ $H_2 = A_4$ est le groupe de Galois de p

SCIENCES SORBONNE UNIVERSITÉ

Partie 3 : Idéaux Galoisiens

$k := \mathbb{Q}$ ou tout corps parfait ; $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ racines $\neq$ de p

$$V_L = \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \mid \sigma \in L\} = L \star \boldsymbol{\alpha} \text{ où } L \subset S_n$$

Idéal galoisien défini par L et $\boldsymbol{\alpha}$: polynômes s'annulant sur V_L

$$\begin{aligned} Id(V_L) &= \{r \in \mathbb{Q}[x_1, \ldots, x_n] \mid r(v) = 0 \ \forall v \in V_L\} \\ &= \{r \in \mathbb{Q}[x_1, \ldots, x_n] \mid \sigma \cdot r(\boldsymbol{\alpha}) = 0 \ \forall \sigma \in L\} \end{aligned}$$

- $\mathfrak{M} = Id(V_{Id_n}) = Id(\{\boldsymbol{\alpha}\})$ est l'idéal maximal des $\boldsymbol{\alpha}$-relations
- $\mathfrak{S} = Id(V_{S_n}) = \bigcap_L Id(V_L)$ est l'idéal des relations symétriques

$$G = Gal_k(\boldsymbol{\alpha}) = \mathrm{Stab}(\mathfrak{M}) = \{\sigma \in S_n \mid \sigma \cdot \mathfrak{M} \subset \mathfrak{M}\}$$

$$k[\alpha_1, \ldots, \alpha_n] = k(\alpha_1, \ldots, \alpha_n) \simeq k[x_1, \ldots, x_n]/\mathfrak{M}$$

car $\mathfrak{M}$ noyau du k-morphisme surjectif d'évaluation : $x_i \mapsto \alpha_i$.

SCIENCES SORBONNE UNIVERSITÉ

Groupe de Galois G et actions sur $k(\boldsymbol{\alpha})$

Soient $\gamma \in k(\alpha_1,\ldots,\alpha_n)$ et $\Gamma,\Gamma' \in k[x_1,\ldots,x_n]$ t.q. $\gamma = \Gamma(\boldsymbol{\alpha}) = \Gamma'(\boldsymbol{\alpha})$

$r = \Gamma - \Gamma' \in \mathfrak{M}$. Si $g \in G = \mathrm{Stab}(\mathfrak{M})$ alors $g \cdot r(\boldsymbol{\alpha}) = 0$

On définit

$$\gamma^g := g \cdot \Gamma(\boldsymbol{\alpha}) = g \cdot \Gamma'(\boldsymbol{\alpha})$$

Pour $\sigma \in S_n$ quelconque ?

Sens : $\sigma \cdot \Gamma := \Gamma(x_{\sigma(1)},\ldots,x_{\sigma(n)})$ et $\sigma \cdot \Gamma(\boldsymbol{\alpha}) := \Gamma(\alpha_{\sigma(1)},\ldots,\alpha_{\sigma(n)})$

$$\begin{array}{rcll} p(x) & = & x^3+1 & \alpha_1 = e^{i\pi} = -1,\ \alpha_2 = e^{i\frac{\pi}{3}},\ \alpha_3 = e^{i\frac{5\pi}{3}} \\ \sigma & = & (2)(1,3) & \gamma = \alpha_2^3 = \alpha_1 \end{array}$$

- $\gamma = \alpha_2^3$: $\Gamma = x_2^3$ on a $\sigma \cdot \Gamma(\boldsymbol{\alpha}) = \alpha^3_{\sigma(2)} = \alpha_2^3 = -1$
- $\gamma = \alpha_1$: $\Gamma' = x_1$ on a $\sigma \cdot \Gamma'(\boldsymbol{\alpha}) = \alpha_{\sigma(1)} = \alpha_3 = e^{i\frac{5\pi}{3}} \neq \sigma \cdot \Gamma(\boldsymbol{\alpha})$

$$r = \Gamma - \Gamma' = x_2^3 - x_1 \in \mathfrak{M} \text{ et } \sigma \cdot r \notin \mathfrak{M} \Rightarrow \sigma \notin G$$

SCIENCES SORBONNE UNIVERSITÉ

Artin (père), 1959

$K = k(\boldsymbol{\alpha})$, (i) corps des racines de $p \in k[x]$, (ii) k parfait
$\Rightarrow$ K est une extension galoisienne de k (i.e. normale et séparable)

Groupe de Galois : $G' := Aut_k(K)$ K-automorphismes fixant k.
$\phi \in G'$: $0 = \phi(p(\alpha_i)) = p(\phi(\alpha_i))$ d'où $\phi(\alpha_i) = \alpha_{\sigma_\phi(i)}$ où $\sigma_\phi \in S_n$
$r \in \mathfrak{M}$: $0 = \phi(r(\boldsymbol{\alpha})) = r(\sigma_\phi(\boldsymbol{\alpha})$ d'où $\sigma_\phi \in G = \mathrm{Stab}(\mathfrak{M})$
inversement : $\sigma \in G \mapsto \phi_\sigma \in G' \Rightarrow$ pour $\boldsymbol{\alpha}$ fixé, abusons : $G = G'$

Correspondance galoisienne

- Si L corps intermédiaire : $k \subset L \subset K$ Alors
  $L = \{\gamma \in K \mid H \cdot \gamma = \{\gamma\}\} = K^H$, où H sous-groupe de G
- H sous-groupe de $G \Longrightarrow k \subset K^H \subset K$
- H normal dans $G \Leftrightarrow L$ ext. normale* et $Gal(L/k) = G/H$
  * L corps des racines d'un pol de $k[x] \Rightarrow$ extension galoisienne
- CP : Théorème de Galois : Si $H := G$ et $L = k$ alors $k = K^G$

Correspondance galoisienne sur les idéaux

Posons $I^L := \mathrm{Id}(L \star (\alpha_1, \ldots, \alpha_n))$, L un sous-ens. de S_n.

Soit $\mathrm{Inj}(I^L, \mathfrak{M})$ ={permutations envoyant I^L dans $\mathfrak{M}$}. Alors

$$Zero(I^L) = \mathrm{Inj}(I^L, \mathfrak{M}) \star (\alpha_1, \ldots, \alpha_n)$$

Théo : L groupe. Alors $G \subset L \Leftrightarrow \mathrm{Inj}(I^L, \mathfrak{M})$ groupe : I^L est "pur"

Théo (PAubry-AV) : I^L pur $\Rightarrow$ engendré par un ens triang séparable.

- Si I, J idéaux radicaux et $\mathfrak{S} \subset I \subset J \subset \mathfrak{M}$ alors I, J galoisiens et

$$G \subset \mathrm{Inj}(J, \mathfrak{M}) \subset \mathrm{Inj}(I, \mathfrak{M}) \subset S_n$$

- Si $H \subset L \subset S_n$ alors il existe $\sigma \in S_n$ t.q.

$$\mathfrak{S} \subseteq I^L \subseteq I^H \subseteq \sigma \cdot \mathfrak{M} = \mathfrak{M}'$$

et $Gal_k(\sigma^{-1} \cdot \boldsymbol{\alpha}) = \mathrm{Stab}(\mathfrak{M}') = \sigma G \sigma^{-1}$
CP : $H \subset G \Leftrightarrow \mathfrak{M} = I^{I_n} = I^H = I^G$

Correspondances galoisiennes

$G = \mathrm{Gal}(\boldsymbol{\alpha})$ où $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ n-uplet des racines $\neq$ de p.
L et H non nécessairement des groupes t.q. $I_n \subset L$.

On a $GL = \mathrm{Inj}(I^L, \mathfrak{M})$ où $GL = \{gl \mid g \in G, l \in L\}$ et

$$I^L = \mathrm{Id}(L \star \boldsymbol{\alpha}) \text{ et } Zero(I^L) = GL \star \boldsymbol{\alpha}$$

$$\begin{array}{ccccccccc}
S_n & \supset & GL & \supset & G & \supset & H & \supset & I_n \\
\mathfrak{S} = I^{S_n} & \subset & I^{GL} = I^L & \subset & \mathfrak{M} = I^G & = & I^H & = & I_n \\
H \text{ groupe} & \Rightarrow & & & k = k(\boldsymbol{\alpha})^G & \subset & k(\boldsymbol{\alpha})^H & \subset & k(\boldsymbol{\alpha})^{I_n}
\end{array}$$

Modules fondamentaux

Tchebotarev, 1950 : $\mathfrak{M}$, idéal galoisien pur, engendré par un ensemble triangulaire formé des "Modules Fondamentaux" :

$$\begin{array}{ccccccccc} k & \subset & k(\alpha_1) & \subset & k(\alpha_1,\alpha_2) & \subset & \cdots & \subset & k(\alpha_1,\ldots,\alpha_n) \\ & & & & \simeq & & & & \\ k & \subset & k[x_1]/F_1 & \subset & k[x_1,x_2]/<F_1,F_2> & \subset & \cdots & \subset & k[x_1,\ldots,x_n]/\mathfrak{M} \end{array}$$

Modules Fondamentaux :

$$\begin{aligned} F_n &= x_n + g_n(x_1,\ldots,x_{n-1}) \\ F_{n-1} &= x_{n-1}^{m_2} + g_{n-1}(x_1,\ldots,x_{n-2}) \\ &\vdots \\ F_2 &= x_2^{m_2} + g_2(x_1,x_2) \\ F_1 &= x_1^{m_n} + g_1(x_1) \end{aligned}$$

$\Rightarrow$ Calculer $G = \mathrm{Gal}_k(\alpha_1,\ldots,\alpha_n) = \mathrm{Stab}(\mathfrak{M})$ (IAbdelJaouad-SO-GR-AV, 2005)

SCIENCES SORBONNE UNIVERSITÉ

Théorème de Galois et effectivité

$$\mathfrak{M} = < F_1(x_1), F_2(x_1, x_2), \ldots, F_n(x_1, \ldots, x_n) >$$

Théorème (Galois) : Soit $\gamma \in k(\boldsymbol{\alpha})$

- $\{\gamma^g \mid g \in G\}$ est l'ens. des racines de $\min_{k,\gamma}$
- $\gamma \in k$ ssi $\gamma^g = \gamma$ pour tout $g \in G$

? Tester si γ est invariant par G. Si oui : ? Valeur de γ dans k.

Théorème (Tchebotarev): Soit $\overline{\Gamma}$ réduction de Γ modulo $F_n(x_n), \ldots, F_1(x_1)$: $\overline{\Gamma} \in k$ ssi $\gamma := \Gamma(\boldsymbol{\alpha}) \in k$ et $\overline{\Gamma} = \gamma$.

$\overline{\Gamma}$: calculer n restes successifs par $F_n(x_n), \ldots, F_2(x_1, x_2), F_1(x_1)$.

$\Rightarrow$ Vérifier que γ est invariant par G et calculer sa valeur dans k.

Galois effectif est résolu... quand les F_i sont calculés ...

SCIENCES SORBONNE UNIVERSITÉ

Tchebotarev : Modules fondamentaux

Algorithme :

- $f_1(x)$ un facteur irr. de $p(x)$ sur $k = k_0$, α_1 racine de f_1
- $f_2(x)$ facteur irr. de p sur $k_1 = k(\alpha_1)$, $\alpha_2 \neq \alpha_1$ racine de f_2
- $f_3(x)$ facteur irr. de p sur $k_2 = k(\alpha_1, \alpha_2)$, α_3 racine de f_3

$$\vdots$$

- $f_n(x)$ facteur irr. de p sur $k_{n-1} = k(\alpha_1, \ldots, \alpha_{n-1})$, α_n racine de f_n.

Posons $F_i \in k[x_1, \ldots, x_i]$ t.q. $F_i(\alpha_1, \ldots, \alpha_i) = f_i(\alpha_i)$ pour $i \in [\![1, n]\!]$.

Alors $F_1, \ldots, F_n$ sont "les" Modules Fondamentaux de $p(x)$:

$$\mathfrak{M} = \langle F_1, \ldots, F_n \rangle$$

Posons $m_i = \prod_i \deg_{x_i}(F_i) = \prod_i \deg_x(f_i)$ pour $i \in [\![1, n]\!]$. Alors

$$\prod_i m_i = \dim_k k(\boldsymbol{\alpha}) = \dim_k k[x_1, \ldots, x_n]/\mathfrak{M} = \#Zero(\mathfrak{M}) = \#G$$

SCIENCES SORBONNE UNIVERSITÉ

Exemple

(i14) factor(x^6+2); (o14) x^6+2

Alors $F_1 = x_1^6+2$, α_1 racine F_1 ; $k_0 = \mathbb{Q}$

Factoriser F_1 sur $k_1 := k(\alpha_1) \simeq k[x_1]/\langle F_1(x_1)\rangle$

(i16) factor$(x^6+2, x1^6+2)$;

(o16) $(x-x1)*(x+x1)*(x^2-x*x1+x1^2)*(x^2+x*x1+x1^2)$

Choix $F_2 = x_2+x_1 \Rightarrow \alpha_2 = -\alpha_1 \in k_2 := k(\alpha_1,\alpha_2) = k_1$

Choix $F_3 = x_3^2 - x_3x_1 + x_1^2$

$\Rightarrow \alpha_3$ racine de $f_3 = F_3(\alpha_1,\alpha_2,x) = x^2 - \alpha_1 x + \alpha_1^2$; $k_3 = k_2(\alpha_3)$

Choix α_4 racine de $f_3 = (x-\alpha_3)(x-\alpha_4) \Rightarrow \alpha_4+\alpha_3 = \alpha_1$

$\Rightarrow F_4 = x_4+x_3-x_1$ et $k_4 := k(\alpha_1,\alpha_2,\alpha_3,\alpha_4) = k(\alpha_1,\alpha_3)$.

Factoriser sur k_4 (SageMath gratuit ou Magma cher):

$$x^2+x\alpha_1+\alpha_1^2 = (x-\alpha_3+\alpha_1)(x+\alpha_3)$$

Choix $F_5 = x_5+x_1-x_3$ et $F_6 = x_6+x_3$

$\mathbb{Q}(\boldsymbol{\alpha}) = \mathbb{Q}(\alpha_1,\alpha_3)$ et $\#G = dim_{\mathbb{Q}}\mathbb{Q}(\boldsymbol{\alpha}) = 6.1.2.1.1.1 = 12$

Problème : Factoriser dans des extensions de degré élevé.

Algorithme GaloisIdeal

$$\mathfrak{S} \subset \cdots \subset \mathrm{Id}(V_L) \subset \cdots \subset \mathfrak{M}$$

Au départ, au pire : $\mathfrak{S}$, pur, engendré par les modules de Cauchy.
Hypothèse de récurrence : $Id(V_L)$ pur, d'injecteur le groupe $L > G$.

Théorème élément primitif (1995) : *Soient un groupe $H < L$, un H-invariant L-primitif $\boldsymbol{\alpha}$-séparable Γ et $\gamma = \Gamma(\boldsymbol{\alpha})$. Alors*

$$Id(V_H) = Id(V_L) + < min_{k,\gamma}(\Gamma) >$$

(2009 : variante, sans hypothèse de séparabilité)
(2007) En déduire efficacement J pur t.q. $Id(V_H) \subset J$

$H = I_n$, $\min_{k,\gamma}$ fact. simple de degré $\#G$ de la résolvante de Galois de degré $n!$ $\Rightarrow$ - $\mathfrak{M} = \mathfrak{S} + < \min_{k,\gamma}(\Gamma) >$
- $k(\boldsymbol{\alpha}) = k(\gamma) \simeq k[x]/\min_{k,\gamma}(x) \simeq k[x_1, \ldots, x_n]/\mathfrak{M}$

$\min_{k,\gamma}$? facteur de $R(p, \Gamma)$ et de la résolvante relative $R_{\Gamma,I}$.

SCIENCES SORBONNE UNIVERSITÉ

Résolvantes relatives

Hyp. I pur, d'injecteur L dans $\mathfrak{M}$ t.q. $G < L$ et $\mathrm{Stab}_L(\Gamma) = H < L$.

Résolvante relative à I par $\Gamma \in k[x_1, \ldots, x_n]$:

$$R_{\Gamma,I} = \prod_{\Theta \in L \cdot \Gamma} (x - \Theta(\alpha_1, \ldots, \alpha_n)) \in k[x]$$

- Résolvante de Lagrange, dite **absolue** : $L = S_n$ et $I = \mathfrak{S}$
- Résolvante de Galois : $H = I_n$, $\Gamma = x_1 + \cdots + nx_n$ et $I = \mathfrak{S}$

Coefficient : polynôme symétrique S de l'orbite $L \cdot \Gamma$ (Viete)
$\Rightarrow S$ invariant par $L \Rightarrow S(\boldsymbol{\alpha})^g = S(\boldsymbol{\alpha})\ \forall g \in G \Rightarrow S(\boldsymbol{\alpha}) \in k$ (Galois)

I triangulaire $\Rightarrow S(\boldsymbol{\alpha})$ est le dernier reste de n divisions euclidiennes successives par les générateurs de I.

La résolvante relative élimine des groupes à être G via la matrice des partitions (groupes) relative à L (idem Partie 1 avec $L = S_n$).

Calculer des résolvantes

Il existe plusieurs méthodes pour calculer $R_{\Gamma,I}$

La naïve : calculer les f.s.e de l'orbite $L \cdot \Gamma$ puis les réduire mod I.

Absolues : générale et particulières dans le module SYM intégré à Maxima (sous SageMath donc)

Quelconques :

- Par élimination, résultants : AV, 1995, Rennert-AV, 1998 (absolues) Aubry-AV, 1998, 2009 (relatives)

- Calculs modulaires, parallèles et théorème chinois des restes : Rennert, 2005 (absolues), Aubry-Val 2010 (relatives)

- Réduction modulo idéal I (AV, Acta Arithm 2008)

- algébro-numériques : Stauduhar, 1973, Abdeljaouad-FB-AV. 2010 (avec certification algébrique)

$\Rightarrow$ détermination du groupe de Galois G par l'Algorithme "GaloisIdeal"

SCIENCES SORBONNE UNIVERSITÉ

Exemple

$p = x^4 - 2$ et G son groupe de Galois $\in \{H_1, H_2, H_3, H_5, H_6\}$

Générateurs de $\mathfrak{S}$, idéal des relations symétriques ?

$p = x^4 - e_1 x^3 + e_2 x^2 - e_3 x + e_4$ avec $e_i = \sum \alpha_1 \cdots \alpha_i$ f.s.e. des racines

Equations symétriques :

$$x_1 + x_2 + x_3 + x_4 = 0 \qquad x_1x_2 + \cdots + x_3x_4 = 0$$

$$x_1x_2x_3 + \cdots + x_2x_3x_4 = 0 \qquad x_1x_2x_3x_4 - (-2) = 0$$

Modules de Cauchy (non symétriques en $x_1, \ldots, x_4$)

$$C_1 := x_1^4 - 2 = p(x_1)$$

$$C_2 := x_2^3 + x_1x_2^2 + x_1^2x_2 + x_1^3 = \frac{C_1(x_1) - C_1(x_2)}{x_1 - x_2}$$

$$C_3 := x_3^2 + x_2x_3 + x_1x_3 + x_2^2 + x_1x_2 + x_1^2 = \frac{C_2(x_1, x_2) - C_2(x_1, x_3)}{x_2 - x_3}$$

$$C_4 := x_4^1 + x_3 + x_2 + x_1$$

Calculs avec les relations symétriques entre les racines de p :

Théo Fond. des Fonctions Symétriques

Modules de Cauchy de p engendrent $\mathfrak{S} = \mathrm{Id}(S_4 \star (\alpha_1, \ldots, \alpha_4))$:

$$C_4 = x_4^1 + x_3 + x_2 + x_1, C_3 = x_3^2 + x_2x_3 + x_1x_3 + x_2^2 + x_1x_2 + x_1^2, C_2 = x_2^3 + x_1x_2^2 + x_1^2x_2 + x_1^3, C_1 = x_1^4 - 2 = p(x_1) \quad .$$

$$1 \cdot 2 \cdot 3 \cdot 4 = \mathrm{Card}(S_4) = dim_{\mathbb{Q}}\mathbb{Q}[x_1, \ldots, x_4]/\mathfrak{S} \qquad (\textit{Algèbre universelle})$$

$s(x_1, \ldots, x_4) = x_1^3 + \cdots + x_4^3$ polynôme symétrique : $S_4 \cdot s = \{s\}$.

$s(\boldsymbol{\alpha}) \in \mathbb{Q}$ selon Galois. Calcul proposé par Cauchy :

$r_4 = Reste(s, C_4, x_4)$, $r_3 = Reste(r_4, C_3, x_3)$, $r_2 = Reste(r_3, C_2, x_2)$,

$$s(\boldsymbol{\alpha}) = Reste(r_2, C_1, x_1) \in \mathbb{Q}$$

Le T.F.F.S est un cas particulier du Théorème de Galois.

SCIENCES SORBONNE UNIVERSITÉ

Exemple (suite)

Données : $G \in \{H_1, H_2, H_3, H_5, H_6\}$ et les Modules de Cauchy

$$x_4^1 + x_3 + x_2 + x_1, x_3^2 + x_2x_3 + x_1x_3 + x_2^2 + x_1x_2 + x_1^2, x_2^3 + x_1x_2^2 + x_1^2x_2 + x_1^3, x_1^4 - 2 \quad .$$

Invariant $\Theta = x_2x_4^2 + x_3x_2^2 + x_4x_1^2 + x_1x_3^2$ de $H_5 = C_4$, groupe test

Résolvante $R = x^2(x^4 + 512)$

Partition $[H_5, G] = ?, 4 \quad \Rightarrow G \in \{H_3 = D_4, H_5 = C_4\}$

Relation $x - 0$ facteur de R : $\alpha_2\alpha_4^2 + \alpha_3\alpha_2^2 + \alpha_4\alpha_1^2 + \alpha_1\alpha_3^2 = 0$

Générateur Théo élément primitif (version 2009) :

$$\mathrm{Id}(D_4 \star \boldsymbol{\alpha}) = \mathrm{Id}(S_4 \star \boldsymbol{\alpha}) + \langle \Theta - 0 \rangle \qquad \text{pur, engendré par}$$

$$f_4 := x_4^1 + x_3, \quad f_3 := x_3^2 + x_1^2, \quad f_2 := x_2^1 + x_1, \quad f_1 := x_1^4 - 2$$

$D_4 \cdot \Gamma = \{\Gamma\} \Rightarrow \gamma := \Gamma(\boldsymbol{\alpha}) \in \mathbb{Q}$ (Théo Galois car $G < D_4$).
$r_4 = Reste(\Gamma, f_4, x_4)$, $r_3 = Reste(r_4, f_3, x_3)$, $r_2 = Reste(r_3, f_2, x_2)$,

$$\gamma = Reste(r_2, f_1, x_1) \in \mathbb{Q}$$

SCIENCES SORBONNE UNIVERSITÉ

Exemple (suite et fin)

$$\mathfrak{S} = \mathrm{Id}(S_4 \star \boldsymbol{\alpha}) \subset I := \mathrm{Id}(D_4 \star \boldsymbol{\alpha}) \subset \mathfrak{M} = \mathrm{Id}(\boldsymbol{\alpha})$$

Soit Γ un C_4-invariant D_4-relatif. $D_4 \cdot \Gamma = \{\Gamma, \Gamma'\}$.
Résolvante relative à I par Γ :

$$R_{\Gamma,I} = (x - \Gamma(\alpha_1, \ldots, \alpha_4))(x - \Gamma'(\alpha_1, \ldots, \alpha_4)) \in \mathbb{Q}[x]$$

On peut choisir Γ t.q. les racines de $R_{I,\Gamma}$ soient simples.
Matrice des partitions de D_4 (à la place de S_4) :
Si $R_{\Gamma,I}$ irréductible $\Rightarrow$ $G = D_4$ et $\mathfrak{M} = Id(D_4 \star \boldsymbol{\alpha})$
Sinon $G = C_4$ et Théo Elt Primitif pour calculer $\mathfrak{M}$

Théo bien connu : facteur linéaire simple $\Rightarrow$ $G < C_4 = \mathrm{Stab}(\Gamma)$

Mixer GaloisIdeal avec Tchebotarev :
$f_3 := x_3^2 + x_1^2$ irreductible sur $k[x_1]/ < f(x_1) >$. Donc $G = D_4$.
Sinon G serait C_4 et un facteur $F_3 = x_3 + g_3(x_1)$ eut été un module fondamental.

L'informatique apporte de nouvelles idées

$p = x^7 - 7x + 3$ $\quad \mathrm{Gal}(p) = G_{168} = \mathrm{Stab}(\mathfrak{M})$ (Cartier).

? 7 relations "triangulaires" f_i engendrant $\mathfrak{M}$ un des $7!/168$ idéaux maximaux de relations.
Expérimentation info.+ nouvelle correspondance galoisienne

Aubry-AV $\Rightarrow \deg_{x_i}(f_i) = 1$ si $i \in \{3,5,6,7\}$
$(deg(f_1), deg(f_2), deg(f_4)) = (7,6,4) \Rightarrow f_1(x_1) = x_1^7 - 7x_1 + 3 = p(x_1)$
Division: $f_2(x_1,x_2) = \frac{f_1(x_2)-f_1(x_1)}{x_2-x_1}$, premier module de Cauchy
Calculer: $f_3(\alpha_1,\alpha_2,x)$:
facteur linéaire de $f_1(x)$ sur $k_2 := \mathbb{Q}(\alpha_1,\alpha_2) \simeq \mathbb{Q}[x_1,x_2]/ < f_1, f_2 >$
Division: $f_4(\alpha_1,\alpha_2,x_4) = \frac{f_2(x_4)}{(x-\alpha_2)\cdot f_3(x_4)}$: calculs faciles dans k_2
Permutations: $f_5(\alpha_1,\alpha_4,x_5) = f_3(\alpha_1,\alpha_4,x_5)$,
$f_6(\alpha_3,\alpha_4,x_6) = f_3(\alpha_3,\alpha_4,x_6)$ et $f_7(\alpha_1,\alpha_6,x_7) = f_3(\alpha_1,\alpha_6,x_7)$

(AV Acta Arith. 2008)

SCIENCES SORBONNE UNIVERSITÉ

Autres méthodes pour calculer $\mathfrak{M}$

- Interpolation Multivariée (Algo Burberger-Möller pour bases de Gröbner): Lederer, 2004 (avec G connu et formules Aubry-Val), McKay-Stauduhar, 1996 (relations primaires)
- Méthode linéaire et p-adic : Yokoyama, 1944, 1999 avecles formules Aubry-Val
- Methodes mixtes avec permutations et divisons euclidiennes (très efficace): Orange-Renault-AV, 2003; AV, 2008.
- Methodes dynamiques : Lombardi et Diaz-Toca, 2009
- "Remontée des vandermondes" : CP pour le cas récalcitrant $Gal = A_n$ (AV 2008)

Mixer toutes les méthodes dans un programme parallèle et collaboratif.

SCIENCES SORBONNE UNIVERSITÉ

Evaluer c'est intersecter avec G

$P = \prod(x - x_i) = x^n + A_1 x^{n-1} + \cdots + A_n$, $K = k(A_1, \ldots, A_n)$
On a $p = P(\boldsymbol{\alpha})$ avec $\mathrm{Gal}_k(p) = G$ sur k (tel $\mathbb{Q}$)

L, H groupes t.q. $H < L$ et Γ t.q $H = \mathrm{Stab}_L(\Gamma)$ et $\gamma = \Gamma(\boldsymbol{\alpha})$

Γ élément primitif de $K(\boldsymbol{x})^H$ sur $K' = K(\boldsymbol{x})^L$ de polynôme minimal
une certaine résolvante "générique" R de degré $[L : H]$

Correspondance galoisienne pour P avec $\mathrm{Gal}_K(P) = S_n$:

$$K = K(\boldsymbol{x})^{S_n} \subset K' = K(\boldsymbol{x})^L \subset \quad K(\boldsymbol{x})^H = K'(\Gamma) \quad \subset k(\boldsymbol{x}) = K(\boldsymbol{x})^{I_n}$$

Si $G < L$ et R "$\boldsymbol{\alpha}$-séparable" $\qquad x_i \mapsto \alpha_i$

$$k = k(\boldsymbol{\alpha})^G \subseteq \quad k(\boldsymbol{\alpha})^{G \cap H} = k(\gamma) \quad \subset k(\boldsymbol{\alpha}) = k(\boldsymbol{\alpha})^G$$

SCIENCES SORBONNE UNIVERSITÉ

Theorie de Galois et algèbre linéaire

k corps parfait ($k = \mathbb{Q}$)
idéal galoisien: $I := \mathrm{Id}(L \star (\alpha_1, \ldots, \alpha_n))$ t.q. $L = \mathrm{Stab}(I) \subset S_n$.

$$R^h_{\Theta,I} = \chi_{\Theta,I}$$

où $h = |\,\mathrm{Stab}_L(\Theta)\,|$ et $\chi_{\Theta,I}$ polynôme carac. de l'endo. multiplicatif de $k[x_1, \ldots, x_n]/I$ induit par Θ : $\overline{P} \mapsto \overline{P \cdot \Theta}$
$\Rightarrow R_{\Theta,I} \in k[x]$ car k corps parfait, alg. linéaire sans utiliser Galois

$\Rightarrow$ Théorèmes de Galois avec $I = \mathfrak{M}$ et $R_{\Theta,I}$ résolvante de Galois

Comme $k(\alpha_1, \ldots, \alpha_n)$ isomorphe à $k[x_1, \ldots, x_n]/\mathfrak{M}$
et $\sqrt{\mathfrak{M}} = \mathfrak{M}$ car les idéaux galoisiens sont radicaux :

$$\#G = \#Zero(\mathfrak{M}) = dim_k(k[x_1; \ldots, x_n]/\mathfrak{M}) = [k(\alpha_1, \ldots, \alpha_n) : k]$$

=> la théorie de Galois peut être vue comme de l'algèbre linéaire

SCIENCES SORBONNE UNIVERSITÉ

Calculs dans $GF(q)$, $Disc(p(x)) \neq \lambda q$

$Gal(p(x) \bmod q) \subset \mathrm{Gal}(p)$ si q ne divise pas $\mathrm{Disc}(p)$

Dedekind (1877) : Les degrés des facteurs irr. de $p(x)$ sur $GF(q)$ sont des longueurs de cycles d'éléments du groupe de Galois G de p, appelés schémas de cycles.

-Tables (pré-calculs) : G. Butler, J. McKay, 1983, Com. in Alg.

- Algorithmes efficaces et parallèles de résolvantes :
N. Rennert, 2004 (absolues) et P. Aubry-AV, 2012 (relatives)

Frobenius (1896) : Soit $(d_1, \ldots, d_r)$ une partition of n, le degré de $p(x)$. Alors la densité relative de l'ensemble des éléments premiers q t.q $p(x) \bmod q$ a une décomposition de type $(d_1, \ldots, d_r)$ est égale à $\frac{1}{G}$ fois le nombres de permutations de G ayant $(d_1, \ldots, d_r)$ comme schéma de cycles.

Ce théorème de densité de Frobenius fut étendu par celui de Tchebotarev en 1923.

Pourquoi l'informatique ?

Résolvantes (absolues) : Théo. Fond. Fonct. Symétriques

Facteurs des polynômes

les (classes de) groupes de permutations

Butler&McKay (trans. $n \leq 11$, 1983) Hulpke ($n \leq 30$, 90)

des invariants $f(x_1, \ldots, x_n)$ pour transformer p

Girstmair (1987) I. Abdeljaouad (1998, GAP)

les matrices de partitions

- Partielles: Berwick ($n = 6$, 1929), Foulkes ($n = 7$, 1931)
- Partielles sur Ordi. : McKay&Soicher ($n \leq 11$, 1983)
- $\forall n$ + Détermination Gal(p) : Arnaudiès-V.(1993)

les matrices de groupes

- Partielles : Berwick ($n = 6$, 1929)
- $\forall n$ + Détermination Gal(p) + Problème inverse (1995)

des "bases de Gröbner" d'idéaux galoisiens (1995)

les résolvantes relatives avec idéaux galoisiens (Aubry-V., 98)

modulairement avec de nombreux entiers => paralléliser

Algébro-numérique

SCIENCES SORBONNE UNIVERSITÉ

Outils de calculs

- Calculs Algébriques

William Frédéric Schelter (1947 - 2001) a développé la version libre sous licence GPL du système de Calcul Formel Maxima comportant les résolvantes dans la bibliothèque Symmetries (AV)

Maple, Mathematica, AXIOM (années 1980) etc ...

- Calculs Numériques
  Octave (libre), Scilab (libre, INRIA), Mathlab
- Calculs Algébriques + Groupes :
  Programmes (années 1970) puis logiciels GAP (libre), Cayley ancêtre de Magma
- Nouvelles générations :
  - SageMath (libre, 2004) : interfaçant tous les autres
  - Mathemagix (libre, 2005)

SCIENCES SORBONNE UNIVERSITÉ

Pour aller plus loin

- *Oeuvres Mathématiques, éditées par la SMF*, E. Galois, Gauthier-Villars, Paris (1897)
- *Réflexions sur la résolution algébrique des équations*, J.-L. Lagrange (1770)
- *Computational Group Theory*, Alexander Hulke : http://www.math.colostate.edu/ hulpke/ (GAP)
- *Inverse Galois theory*, H. Matzat et G. Malle (1999) (Galois inverse)

Nombreuses références et exemples dans :

- *Etude des relations entre les racines des polynômes*, A.V., Acta Arithmetica (2008)
- *Résolvantes, groupe de Galois et Idéaux galoisiens*, A.V., Hal-00421725 (2009)

SCIENCES SORBONNE UNIVERSITÉ