La Théorie de Galois en Informatique

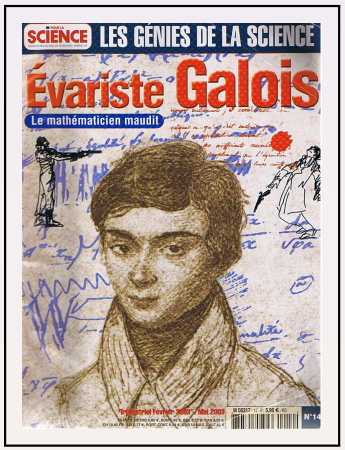
Anniversaire du Bicentenaire de la Naissance d'Évariste Galois

Annick Valibouze

LIP6 - LSTA - Université Pierre et Marie Curie, Paris 6, France

Bourg-la-Reine (Hauts-de Seine - France)

Samedi 5 Novembre 2011



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

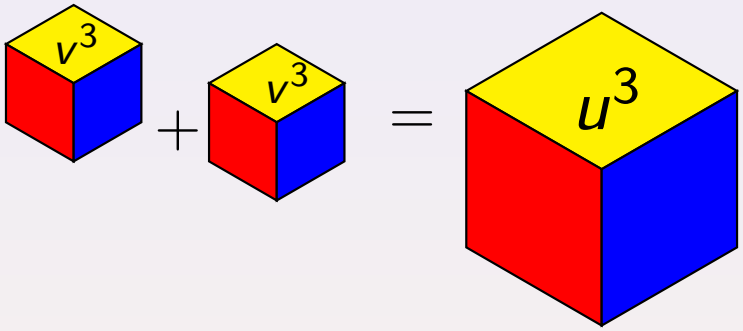
- Problème non algèbrique

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

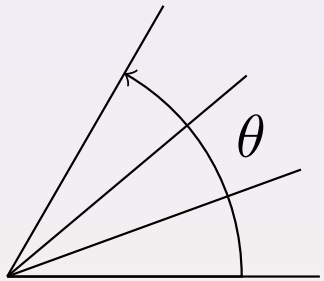
Ferdinand von Lindemann (1882) : transcendance de π

- Problèmes algèbriques

Duplication du cube



Trisection de l'angle θ



$\theta = 60°$
$x = cos(\theta/3)$

- Mise en équations avec Descartes (1596) :

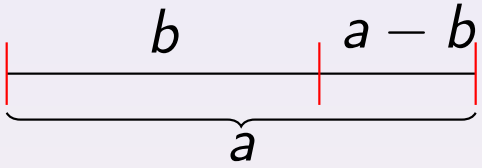
$x^3 - 2v^3 = 0$ $\qquad$ $8x^3 - 6x - 1 = 0$

- 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 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$                        = φ = (1+√5)/2
In [10]: sol_numer:  float(sol_alg);
Out[10]: 1.618033988749895 approximation numérique φ̃ de φ
In [11]: subst(sol_alg,x,p);                           p(φ) = ?
Out[11]: 0                                             p(φ) = 0
In [12]: subst(sol_numer,x,p);                         p(φ̃) = ?
Out[12]: 0.0          Résultat assez proche de 0 : p(φ̃) ≃ 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
```

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 racines $\alpha_1, \alpha_2, \ldots, \alpha_n$:

$$p = a_n(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$$

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.

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

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

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

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) Cela s'arrêtera au delà du degré 4

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

Théorème Galois : Critère déterminant la résolution par radicaux

Résolution et Informatique

Formules	(XVI-ième S.) Pour tout polynôme de degré inférieur à 4
Algo	(XVIII-ième S.) Pour tout polynôme de degré inférieur à 4
Idée	Lagrange (1770) Rabaisser le degré en transformant par
Outil	des Résolvantes $\Rightarrow$ calculs
Outil	Galois : groupe du polynôme $\Rightarrow$ calculs
Théorie	Polynôme résoluble/radicaux ssi groupe résoluble $\Rightarrow$ calculs
Théorème	Cayley (1861) Sa résolvante teste la résolution en degré 5
Outils	Artin (1944) Extensions galoisiennes, automorphismes ...
Théorie	abstraite $\Rightarrow$ Correspondance galoisienne
Calculs	Dummit (1991) Résoudre les équations résolubles en degré 5
Théorème	Arnaudiès-V. (1993) Groupe de Galois avec des résolvantes
Calculs	Hagedorn (2000) Résoudre les équations résolubles en degré 6

Théorie de Galois à la Galois

- $p = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \quad a_i \in \mathbb{Z},\ n \in \mathbb{N}, a_n \neq 0$
  Racines (inconnues et distinctes) : $\alpha_1, \alpha_2, \quad , \alpha_n$.

- Définition de la Résolvante de Galois
  Polynôme R dont les racines sont les $n! = n(n-1)(n-2)\cdots 1$ permutés distincts de $V_1 = \alpha_1 + 2\alpha_2 + 3\alpha_3 + \cdots + n\alpha_n$
  - permutation $(1,2)$: $(1,2).V_1 = \alpha_2 + 2\alpha_1 + 3\alpha_3 + \quad + n\alpha_n$
  - R se factorise en des polynômes de même degré e.

- Définition du Groupe de Galois $\mathrm{Gal}(p)$ de p
  Ensemble des e permutations qui échangent $V_1, \ldots, V_e$, les racines d'un des facteurs de R.

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

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
  - $p = x^3 - 6$
    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) : 3!=6 éléments $\Rightarrow$ racines indiscernables

Principaux Défis en Théorie de Galois

- **Détermination du groupe de Galois** $\mathrm{Gal}(p)$ du polynôme p
- **Test à zéro** d'expressions polynomiales en les racines de p :

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

- **Problème inverse de Galois** : *Soit G un groupe*
  Existence et Calcul d'un polynôme p t.q. $G = \mathrm{Gal}(p)$

Pierre Cartier, il y a 20 ans, me montrait comment le groupe à 168 éléments est réalisé par le polynôme $p = x^7 - 7x + 3$ il utilisait la résolvante de p par $x_1 + x_2 + x_3$

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

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. $36_3 =$

+	+	+	+	−	−
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*,

Avec le logiciel GAP - 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	$\mathfrak{A}_4$	12
H_3	$\mathcal{D}_4$	8
H_4	$Id \times S_3$	6
H_5	$\mathcal{C}_4 = (\mathbb{Z}/4\mathbb{Z})$	4
H_6	$(\mathbb{Z}/2\mathbb{Z})^2$	4
H_7	$(\mathbb{Z}/2\mathbb{Z})^2$	4
H_8	$\mathfrak{A}_3 \times S_1$	3
H_9		2
H_{10}	$S_1 \times S_1 \times S_2$	2
H_{11}	Id_4	1

Intérêt des invariants (primitifs)

La résolvante résulte d'une transformation du polynôme $p(x)$ de groupe de Galois G par $f(x_1, \ldots, x_n)$ un polynôme multivarié invariant par les permutations d'un groupe H et uniquement par celles-ci.

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

Chaque groupe H est un **testeur** du groupe de Galois G

Invariant (primitif) : Un polynôme multivarié f qui identifie H

? Calculer un invariant primitif f de H afin d"'algébriser le test" sur le polynôme p

Invariants des groupes en degré 4

L'indice du groupe est le degré de la résolvante

Noms	Indices	Invariants primitifs
H_1	1	1
H_2	2	$(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4)$
H_3	3	$x_1x_2+x_3x_4$
H_4	4	x_1
H_5	6	$(x_1-x_2)(x_2-x_3)(x_3-x_4)(x_4-x_1)$
H_6	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}	24	$x_1+2x_2+3x_3$ ou $x_1x_2^2x_3^3$

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

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

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
- H et G deux groupes (connus sous GAP)
- $f(x_1, \ldots, x_n)$ un invariant primitif de H (calculé avec GAP)

Outils programmables (et implantés !) :
- Une certaine partition d'entiers $[H, G]$, précalculée (GAP, 1993)
- Résolvante séparable R de p par f (Maxima, 1988)

Théorème (Arnaudiès-V., 1993)

1- $G = \mathrm{Gal}(p)$ *implique* $[H, G] =$ *degrés des facteurs de* R

2- $\mathrm{Gal}(p)$ *est ainsi déterminable en tout degré* n

Matrice des partitions (absolue) en degré 4

Première Colonne : Testeurs

Première Ligne : Candidats à être le groupe de Galois

Ligne H_i - Colonne H_j = partition $[H_i, H_j]$

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

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

	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}

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)); testeur = H_2

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)); testeur = H_3

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

Théorème fondamental de Galois

Résolvante: discrimine les groupes et produit des relations

- $p = x^4 - 2$ et G son groupe de Galois $\in \{H_1, H_2, H_3, H_5, H_6\}$
- Coefficients de $p \Rightarrow$ équations symétriques des racines :

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 &= 0 \quad \alpha_1\alpha_2 + \cdots + \alpha_3\alpha_4 = 0 \\ \alpha_1\alpha_2\alpha_3 + \cdots + \alpha_2\alpha_3\alpha_4 &= 0 \quad \alpha_1\alpha_2\alpha_3\alpha_4 = 0 \end{aligned}$$

- Modules de Cauchy engendrent les relations symétriques

$$\begin{aligned} & x_4^1 + x_3 + x_2 + x_1 \\ & x_3^2 + x_2x_3 + x_1x_3 + x_2^2 + x_1x_2 + x_1^2 \\ & x_2^3 + x_1x_2^2 + x_1^2x_2 + x_1^3 \\ & x_1^4 - 2 \end{aligned}$$

=> Calculer avec les "expressions symétriques" des racines

Si $G = H_1 = S_4$: racines indiscernables et aucune autre relation

Théorème fondamental de Galois

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

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

Invariant $f = x_2x_4^2 + x_3x_2^2 + x_4x_1^2 + x_1x_3^2$ de $H_5 = C_4$, le testeur

Résolvante $R = x^2(x^4 + 512)$

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

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

Relations Ensemble engendrant l'idéal galoisien stabilisé par $H_3 = D_4$

$$x_4^1 + x_3, \quad x_3^2 + x_1^2, \quad x_2^1 + x_1, \quad x_1^4 - 2$$

=> On s'approche du théorème de Galois

=> Calculer exactement des résolvantes relatives à H_3

Conclure - Matrices des partitions : résolvantes relatives et extensions

- $Gal(p \bmod EntierPremier) \subset \mathrm{Gal}(p)$ (pas systématique)

=> $G = H_3$ et Test à zéro

L'informatique apporte de nouvelles idées

$p = x^7 - 7x + 3$ Groupe de Galois à 168 éléments (Cartier).

? 7 relations "minimales" r_i engendrant toutes les relations.

Expérimentation info. + nouvelle correspondance galoisienne
$\Rightarrow$ des deux relations r_1, r_3 se déduisent rapidement les autres

$r_1(x_1) = x_1^7 - 7x_1 + 3$ connue $r_3(x_1, x_2, x_3)$ à calculer

Division: $r_2(\alpha_1, x_2) = \frac{r_1(x_2)}{x_2 - \alpha_1}$ $r_4(\alpha_1, \alpha_2, x_4) = \frac{r_2(x_4)}{(x-\alpha_2).r_3(x_4)}$
Permutation: $r_5(\alpha_1, \alpha_4, x_5) = r_3(\alpha_1, \alpha_4, x_5)$
$r_6(\alpha_3, \alpha_4, x_6) = r_3(\alpha_3, \alpha_4, x_6)$ $r_7(\alpha_1, \alpha_6, x_7) = r_3(\alpha_1, \alpha_6, x_7)$

Gal(p) *se définit aussi comme l'ensemble des permutations envoyant une relation sur une autre relation*

Corps de Galois et Codes Correcteurs d'Erreurs

Emission un mot $m = (1, 0, 0, 1)$ **Réception** m ... ou pas

Information supplémentaire : $c = m + r = (1, 0, 0, 1, 1, 0)$
Emission c qui appartient au Code car satisfait une propriété
Réception un mot d qui appartient ou non au Code .

Codes cycliques : Corps de Galois $GF(2)$ à deux éléments $\{0, 1\}$.
- Choisir p un facteur de degré n de $x^m - 1$ sur $GF(2)$
- Corps de Galois $GF(2^n)$ à 2^n éléments contenant les racines de p
- Groupe de Galois de p : éléments de Frobenius.
- **Mots du Code** : multiples de p

$$c = 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x + 0$$

Détecter les erreurs : d multiple de p ... ou pas
Corriger : mot du Code le plus proche de d

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 ($n = 7$, 31)
- 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)

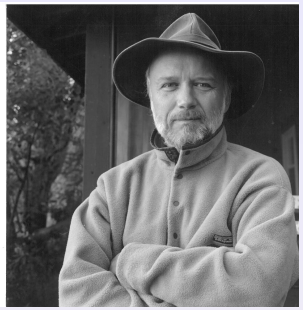
les résolvantes relatives avec idéaux galoisiens (Aubry-V., 98)

modulairement avec de nombreux entiers => paralléliser

Algébro-numérique

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 sa bibliothèque Symmetries (V.)

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 :
  - Sage (libre, 2004) : interfaçant tous les autres
  - Mathemagix (libre, 2005)

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)
- *La quadrature du cercle et le nombre* π, A. Krop, Ellipses (2005)
- *Computational Group Theory*, Alexander Hulke : http://www.math.colostate.edu/ hulpke/ (GAP)
- *Inverse Galois theory*, H. Matzat et G. Malle (1999) (Galois inverse)
- *Algebraic Coding Theory*, Elwyn R. Berlekamp (Revised 1984) (Corps finis de Galois)
- *Théorie de Galois Constructive*, A. Valibouze, HDR-Université Paris VI, UPMC (1994) (Galois direct et inverse)
- *Etude des relations entre les racines des polynômes*, A. Valibouze, Acta Arithmetica (2008) (Galois direct)