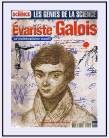
Galoiseries

Annick Valibouze

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

Groups and Langages, en l'honneur de Toni Machi, Rome 2010



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

$a_i \in k$, a field

n distinct roots $(\alpha_1, \ldots, \alpha_n) = \underline{\alpha}$ in an algebraic closure of k

Beginning of history since Lagrange

First goal: Exprime the roots by radicals

- more than 2000 years before JC: $n = 2$
- antiquity : some equations of degree $n = 3$
- Scipione del Ferro, 1500 : $x^3 + px - q$ (Tartaglia, 1535 and Cardan, 1545)
- Ferrari, 1540 and Cardan, 1945 : degree 4
- Lagrange, 1770, introduced the Resolvent in order to unified the solvability methods and to prove that it is not possible to solve each polynomial by radicals from degree 5.

Since Lagrange we have a new objet clearly defined

the (Lagrange) resolvent

He writes

Cet examen aura un double avantage ; d'un côté il servira à répandre une plus grande lumière sur les résolutions connues du troisième et du quatrième degré ; de l'autre il sera utile à ceux qui voudront s'occuper de la résolution des degrés supérieurs, en leur fournissant différentes vues pour cet objet et en leur épargnant surtout un grand nombre de pas et de tentatives inutiles.

Other reference : Vandermonde, 1771, "Mémoire sur la résolution des équations" (resolvents, relations, permutations, solvabily)

The Lagrange Resolvent : idea

Resolvent : an univariate polynomial $R = R_\Theta$ resulting of an algebraic transformation Θ of f.

Dihedral resolvent $deg(f) = n = 4$ and $\Theta = x_1x_2 + x_3x_4$ and

$$R = (x - (\alpha_1\alpha_2 + \alpha_3\alpha_4))(x - (\alpha_1\alpha_3 + \alpha_4\alpha_2))(x - (\alpha_1\alpha_4 + \alpha_3\alpha_2))$$

Ferrari: solve degree $n = 4$ from the solvability in degree $3 = deg(R)$

Idea of Lagrange (and Vandermonde): from degree 5, it is not clear that we can decrease the degree for each polynomial by a resolvent.

The Vandermonde-Lagrange resolvent for the solvability: the $n!$ roots of R are

$$\epsilon\alpha_{i_1} + \epsilon^2\alpha_{i_2} + \cdots + \epsilon^n\alpha_{i_n}$$

where $\epsilon^n = 1$ and $\{i_1, i_2, \ldots, i_n\} = \{1, \ldots, n\}$.

The Lagrange resolvent : coefficients

Why the coefficients of R_Θ belong to k like those of f in $k[x]$?

Considere the symmetric orbit of $\Theta = x_1x_2 + x_3x_4$:

$$S_n.\Theta = \{\Theta_1 = x_1x_2 + x_3x_4, \Theta_2 = x_1x_3 + x_4x_2, \Theta_3 = x_1x_4 + x_3x_2\}$$

Evaluations in roots of f => roots of R:

$$\theta_1 = \Theta_1(\alpha_1, \ldots, \alpha_4) = \alpha_1\alpha_2 + \alpha_3\alpha_4 \quad , \theta_2 = ..., \theta_3 = ...$$

$$R = (x - \theta_1)(x - \theta_2)(x - \theta_3)$$

The coefficients of R are symmetric polynomials of its roots:

$$R = x^3 - (\theta_1 + \theta_2 + \theta_3)x^2 + (\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3)x - \theta_2\theta_2\theta_2$$

then symmetric in roots of f too.
By **fondamental theorem of symmetric functions** the coefficients of R are algebraic expressions in coefficients of f.

The Lagrange Resolvent : computation

How computes Lagrange resolvents ? Many effective methods. The first methods (which are optimised now) given by Lagrange:

- By recursive elimination method:
  $W := x - \Theta$, For i:=1 to n do W :=Resultant($f(x_i), W, x_i$).
  R^m is a factor of W computable by some others recursive elimination methods.
- By computing power functions of roots of R:

  $$p_i = \theta_1^i + \theta_2^i + \theta_3^i$$

  symmetric in the roots of f and deduce the coefficients of R by Girard-Newton relations.

General and particular resolvents are available in Maxima (AV)
(i3) f:$x^4 + a3 * x^3 + a2 * x^2 + a1 * x + a0$;
(i9) resolvante_diedrale(f,x);
(o9) $x^3 - a2 * x^2 + (a1 * a3 - 4 * a0) * x - a0 * a3^2 + 4 * a0 * a2 - a1^2$

Lagrange proposes to describe the transformation Θ s.t. the invariance by permutations appear in its expression.
For example, $\Theta((x1, x3), \dots)$ if Θ leaves unchanged when x_1, x_3 are permuted. Actuallly, there are generators of the permutation group H leaving Θ invariant

Definition: $H < L$. Θ L-primitive H-invariant if $Stab_L(\Theta) = H$.

He computes the degree of the resolvent: $n!$ divided by the order of $Stab(\Theta)$ (the group H). It is the index of H in S_n.
Origine of the classical Lagrange formulae: $\mid H \mid .[L : H] = \mid L \mid$.

Actually, the (absolute) resolvent of f by Θ is

$$R_\Theta = \prod_{\sigma \in S_n/H} (x - \sigma.\Theta(\underline{\alpha}))$$

Permutations in Vandermonde

Also in Θ and permutations leaving invariant the relations among the roots α_i.

Abel, 1824-Ruffini, 1799: $n = 5$, the general equation is not solvable by radical

Galois, 1831: group of the equation $f = 0$, the Galois group of f

Galois resolvent (actually, Lagrange used it before)

$$\Theta = t_1 x_1 + \cdots + t_n x_n$$

$t_i \in k$ pairwise distincts s.t. the n! roots of R_Θ are pairwise distinct

R factorises in k-irreducible factors of same degree g and there is a group G of order g which "exchanges" the roots of each factor.

Lagrange (Galois) Theorem:

$$R(\theta) = 0 => \alpha_i = p(\theta)$$

p univariate polynomial with $deg(p) < g$, the order of G
i.e. θ is a primitive element of the field of roots of f

- f is solvable by radicals iff G is a solvable group
- an algebraic expression γ in roots of f over k belongs to k iff γ is invariant by G: $G.\gamma = \{\gamma\}$

- f is solvable by radicals iff G is a solvable group
- an algebraic expression γ in roots of f over k belongs to k iff γ is invariant by G: $G.\gamma = \{\gamma\}$

Permute only with the Galois group G

$G.\gamma = \{\gamma\}$ makes sens ?

$\Gamma \in k[x_1, \ldots, x_n]$, $\gamma = \Gamma(\alpha_1, \ldots, \alpha_n)$ and $\sigma \in S_n$, a permutation

It is possible to write

$$\sigma.\Gamma(\underline{\alpha}) = \Gamma(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$$

but $\sigma.\gamma$ makes no sens if $\sigma \notin G$.

$$f(x) = x^3 + 1 \qquad \alpha_1 = e^{i\pi} = -1,\ \alpha_2 = e^{i\frac{\pi}{3}},\ \alpha_3 = e^{i\frac{5\pi}{3}}.$$

let $\tau = (2)(1,3)$ and $\gamma = \alpha_2^3 = \alpha_1$ ($\Gamma = x_2^2$ or $\Gamma = x_1$)

$$\alpha_{\tau(2)}^3 = \alpha_2^3 = -1 \neq \alpha_{\tau(1)} = \alpha_3 = e^{i\frac{5\pi}{3}}$$

$(2)(1,3) \notin G$ and $G \neq S_n$

G is the set s.t. an action can be defined (Indetermination theory)

Artin (father), 1959

Let $K = k(\underline{\alpha})$, the field of roots of $f \in k[x]$, k, perfect (think $k = \mathbb{Q}$)

Galois group $G := Gal(K/k)$: automorphisms of K, leaving k invariant.
Each element of G is entirely defined by an auto-bijection of $\{\alpha_1, \ldots, \alpha_n\}$.

The galoisian correspondence

- Let L be an intermediate field: $k \subset L \subset K$.
  Then $L = \{\gamma \in K \mid H.\gamma = \{\gamma\}\} = K^H$ where H subgroup of G
- $H < G \Rightarrow k \subset K^H \subset K$.
- H normal in $G \Leftrightarrow L$ is the field of roots of a polynomial of $k[x]$ with $Gal(L/k) = G/H$.

Not constructive point of view

but usefull to anderstand and prove many things as Galois Theorem:
$k = k(\underline{\alpha})^G$ or $G = Stab_G(k(\underline{\alpha}))$

Let $K = k(\underline{\alpha})$, the field of roots of $f \in k[x]$, k, perfect (think $k = \mathbb{Q}$)

Galois group $G := Gal(K/k)$: automorphisms of K, leaving k invariant.
Each element of G is entirely defined by an auto-bijection of $\{\alpha_1, \ldots, \alpha_n\}$.

The galoisian correspondence

- Let L be an intermediate field: $k \subset L \subset K$.
  Then $L = \{\gamma \in K \mid H.\gamma = \{\gamma\}\} = K^H$ where H subgroup of G
- $H < G \Rightarrow k \subset K^H \subset K$.
- H normal in $G \Leftrightarrow L$ is the field of roots of a polynomial of $k[x]$ with $Gal(L/k) = G/H$.

Not constructive point of view
but usefull to anderstand and prove many things as Galois Theorem:
$k = k(\underline{\alpha})^G$ or $G = Stab_G(k(\underline{\alpha}))$

Artin (father), 1959

Let $K = k(\underline{\alpha})$, the field of roots of $f \in k[x]$, k, perfect (think $k = \mathbb{Q}$)

Galois group $G := Gal(K/k)$: automorphisms of K, leaving k invariant.
Each element of G is entirely defined by an auto-bijection of $\{\alpha_1, \ldots, \alpha_n\}$.

The galoisian correspondence

- Let L be an intermediate field: $k \subset L \subset K$.
  Then $L = \{\gamma \in K \mid H.\gamma = \{\gamma\}\} = K^H$ where H subgroup of G
- $H < G \Rightarrow k \subset K^H \subset K$.
- H normal in $G \Leftrightarrow L$ is the field of roots of a polynomial of $k[x]$ with $Gal(L/k) = G/H$.

Not constructive point of view
but usefull to anderstand and prove many things as Galois Theorem:
$k = k(\underline{\alpha})^G$ or $G = Stab_G(k(\underline{\alpha}))$

G solvable group:

$$G = G_0 < G_1 < G_2 < \cdots < G_r =< 1 >$$

s.t. G_{i-1}/G_i cyclic of order prime n_i
if k_0 contains a primitive n-th root of unity then

$$k_0 = k \subset \cdots k_{i-1} \subset k_i \cdots \subset k(\alpha_1, \ldots, \alpha_n) = k_r$$

$k_i = k_{i-1}(b) = k(\underline{\alpha})^{G_i}$ where $b^{n_i} = a$ with $a \in k_{i-1}$

Goal find b and $x^{n_i} - a$ its minimal polynomial over k_{i-1} .

In polynomial time: Landau-Miller, 1981 (Imprimitivity blocs of G)

$n = 5$: Cayley, 1861, Arnaudiès, 1976, Dummit, 1991, ...
The meta-cyclic group M_5 is the maximal solvable group.
The Cayley resolvent associated to M_5 is always square free and has a linear factor iff G is solvable (i.e. a subgroup of M_5)

$n = 6$: Hagedorn, 2000.

Alexander Hulpke example: $x^6 - 3x^2 - 1$

sage: gp.polgalois('$x^6 - 3 * x^2 - 1$')
$[12, 1, 1, '' A_4(6) = [2^2]3'']$

$$G = G_0 < G_1 < G_2 < G_3 =< 1 >$$

$n_1 = 3, n_2 = n_3 = 3.$

$$k \subset k_1 = k(\alpha_1 + \alpha_2) \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) = k(\underline{\alpha})$$

$G_1 = Stab_G(\alpha_1 + \alpha_2)$ and $G_2 = Stab_G(\alpha_1)$
$\theta = \alpha_1 + \alpha_2$ is a root of a factor of degree 3 of the resolvent $R_{x_1+x_2}$ => solvable.
α_1 is a root of $f_1 = x^2 - 3/4\theta + 2$, a factor of f over $k_1 = k(\theta)$ => solvable.
Replace θ by its expression by radicals in the expression of α_1
=> Finish for α_1.

On the other Galois result

Γ, a polynomial in $x_1, \ldots, x_n$ over k and $\gamma = \Gamma(\underline{\alpha})$.

Galois Theorem: $\gamma \in k$ *iff* γ *is invariant by* G *(i.e.* $G.\gamma = \{\gamma\}$*)*

$f = x^6 - 3x^2 - 1$

- *An algebraic expression in roots:* $\gamma = \alpha_1 + \cdots + \alpha_6$
  $\Gamma = x_1 + \cdots + x_6$ *symmetric polynomial => invariant by* G
  => γ *belongs to* k*. We have* $\gamma = 0$ *(-coefficient of* x^5 *in* f*).*
  Easy : Fundamental Theorem of symmetric functions !
  Conversely : $\gamma = 0 \in k$ *=>* γ *invariant by* G*.*
- *Another expression:* $\gamma = \alpha_1^6 - 3\alpha_1^2 - 1 = f(\alpha_1)$; $\Gamma = f(x_1)$
  $\sigma.\Gamma(\alpha_1) = f(\alpha_{\sigma(1)}) = f(\alpha_i) = 0$ *for* $\sigma \in S_n$
  => Γ *symmetric relation; Not symmetric polynomial!*
  => γ *invariant by* G *=>* $\gamma \in k$ *(*$\gamma = 0$*)*
- *Another expression :* $\gamma = \alpha_1 + \alpha_3$*. What about ???*

Recall : $\gamma = \Gamma(\underline{\alpha})$, $\Gamma \in k[x_1, \ldots, x_n]$

- Problem 1: $G.\gamma = \{\gamma\}$?
  If $G.\gamma = \{\gamma\}$ how to compute the value γ in k ?
  i.e. compute u in k s.t. $\Gamma - u$ is a relation.

  Difficulties: α_i are unknown : $\alpha_1 + \alpha_3$ is not $\alpha_1 + \alpha_2$.
  How define the action of G on the roots of f ?
- Problem 2 Choose usefull resolvents to determine the Galois group
- Problem 3 Compute resolvents (absolute and relative)

Constructive version of Galois Theorems

Recall : $\gamma = \Gamma(\underline{\alpha})$, $\Gamma \in k[x_1, \ldots, x_n]$

- Problem 1: $G.\gamma = \{\gamma\}$?
  If $G.\gamma = \{\gamma\}$ how to compute the value γ in k ?
  i.e. compute u in k s.t. $\Gamma - u$ is a relation.

  Difficulties: α_i are unknown : $\alpha_1 + \alpha_3$ is not $\alpha_1 + \alpha_2$.
  How define the action of G on the roots of f ?
- Problem 2 Choose usefull resolvents to determine the Galois group
- Problem 3 Compute resolvents (absolute and relative)

Recall : $\gamma = \Gamma(\underline{\alpha})$, $\Gamma \in k[x_1, \ldots, x_n]$

- Problem 1: $G.\gamma = \{\gamma\}$?
  If $G.\gamma = \{\gamma\}$ how to compute the value γ in k ?
  i.e. compute u in k s.t. $\Gamma - u$ is a relation.

  Difficulties: α_i are unknown : $\alpha_1 + \alpha_3$ is not $\alpha_1 + \alpha_2$.
  How define the action of G on the roots of f ?
- Problem 2 Choose usefull resolvents to determine the Galois group
- Problem 3 Compute resolvents (absolute and relative)

Solve Problem 3: Computation of Relative resolvents

L a group containing G, $H = Stab_L(\Theta)$
We have $L.\Theta$ instead of $S_n.\Theta$.

L-Relative resolvent of $\underline{\alpha}$ by Θ

$$R_{\Theta,L} = \prod_{\Psi \in L.\Theta} (x - \Psi(\underline{\alpha}))$$

Coefficients of $R_{\Theta,L}$ invariant by L => by G => belong to k.
How to compute algebraically $R_{\Theta,L}$ when $L \neq S_n$?

First (expensive) solution: with some primitive elements (Arnaudies-AV, 1993)
We will use galoisian ideal (see later)

Interest of relative resolvents $R_{\Theta,L}$ is a factor over k of R_{Θ,S_n}
=> decrease time and space during the computation and precise the order of roots.

Solve Problem 2 Determination of the the Galois group

- f irreductible Berwick ($n = 5, 6$, 1915, 1929), Foulkes ($n = 7$, 1931), Jordan-Stauduhar (1870,1975, graph of subgroups, implemented in GP-Pari by Eichenlaub), McKay-Soicher ($n \leq 7$, 1981, implemented in Maple by Soicher), .
- General case
  - The degrees of the factors of resolvents depends only on G and H and the partition matrice of these degrees determine G (Arnaudiès-AV, 1993).
  - The Galois groups of the factors of $R_{\Theta,L}$ depends only on G and H ; the groups matrice determine rapidly G and is usefull for the inverse Galois problem (AV, 1995)
- Frobenius Theorem: the degrees of the factors of $f \bmod p$ give a cycle type of G ; the Galois group of $f \bmod p$ is a subgroup of G (see Density Tcheborarev Theorem and McKay-Butler, 1983, McKay, 1979).

To solve Problem 2, absolute resolvents ($L = S_n$) are sufficient but the computation is expensive.

Solve Problem 2 Determination of the the Galois group

- f irreductible Berwick ($n = 5, 6$, 1915, 1929), Foulkes ($n = 7$, 1931), Jordan-Stauduhar (1870,1975, graph of subgroups, implemented in GP-Pari by Eichenlaub), McKay-Soicher ($n \leq 7$, 1981, implemented in Maple by Soicher), .
- General case
  - The degrees of the factors of resolvents depends only on G and H and the partition matrice of these degrees determine G (Arnaudiès-AV, 1993).
  - The Galois groups of the factors of $R_{\Theta,L}$ depends only on G and H ; the groups matrice determine rapidly G and is usefull for the inverse Galois problem (AV, 1995)
- Frobenius Theorem: the degrees of the factors of $f \bmod p$ give a cycle type of G ; the Galois group of $f \bmod p$ is a subgroup of G (see Density Tcheborarev Theorem and McKay-Butler, 1983, McKay, 1979).

To solve Problem 2, absolute resolvents ($L = S_n$) are sufficient but the computation is expensive.

Solve Problem 2 Determination of the the Galois group

- f irreductible Berwick ($n = 5, 6$, 1915, 1929), Foulkes ($n = 7$, 1931), Jordan-Stauduhar (1870,1975, graph of subgroups, implemented in GP-Pari by Eichenlaub), McKay-Soicher ($n \leq 7$, 1981, implemented in Maple by Soicher), .
- General case
  - The degrees of the factors of resolvents depends only on G and H and the partition matrice of these degrees determine G (Arnaudiès-AV, 1993).
  - The Galois groups of the factors of $R_{\Theta,L}$ depends only on G and H ; the groups matrice determine rapidly G and is usefull for the inverse Galois problem (AV, 1995)
- Frobenius Theorem: the degrees of the factors of $f \bmod p$ give a cycle type of G ; the Galois group of $f \bmod p$ is a subgroup of G (see Density Tcheborarev Theorem and McKay-Butler, 1983, McKay, 1979).

To solve Problem 2, absolute resolvents ($L = S_n$) are sufficient but the computation is expensive.

Solve Problem 1: Cauchy, 1840

Toni Machi showed me this fundamental paper
The Cauchy moduli:

$$C_n = f(x_n), C_{n-1} = \frac{C_n(x_{n-1}) - C_n(x_n)}{x_{n-1} - x_n}, \dots$$

C_i is a polynomial in variables $x_1, \dots, x_i$ with degree i in x_i.
Close formulae : Machi-AV, 1991

Reduction of Γ modulo the Cauchy moduli:
Compute the remainder p_{n-1} of $\Gamma = p_n$ by $C_n(x_n)$, the remainder p_{n-2} of p_{n-1} by $C_{n-1}(x_{n-1})$, $\dots$, the remainder p_1 of p_2 by $C_1(x_1)$.

Cauchy Theorem Γ *symmetric polynomial =>* $p_1 \in k$ *and* $\gamma = p_1$.

Theorem $\mathcal{S}$ *the set (an ideal) of symmetric relations is generated by the Cauchy moduli (a Gröbner basis)*

$$\Gamma - p_1 \in \mathcal{S} \text{ and } \gamma = p_1(\underline{\alpha})$$

Nullestellenstazt (Hilbert): $\Gamma \in \mathcal{S}$ iff $p_1 = 0$

Solve Problem 1: Tchebotarev, 1950

We search a constructive method for Galois theorem.
Toni Machi showed me this fundamental book of Tchebotarev

- $f_1(x)$ a factor of $f(x)$ over $k = k_0$, α_1 a root of f_1
- f_2 a factor of f over $k_1 = k(\alpha_1)$, $\alpha_2 \neq \alpha_1$ a root of f_2
- f_3 a factor of f over $k_2 k(\alpha_1, \alpha_2)$, α_3 a root of f_3

$\vdots$

- f_n a factor of f over $k_{n-1} = k(\alpha_1, \ldots, \alpha_{n-1})$, α_n a root of f_n.

F_i multivariate polynomial s.t. $F_i(\alpha_1, \ldots, \alpha_i) = f_i(\alpha_i)$.
$F_1, \ldots, F_n$: fundamental moduli.

Let p_1 the reduction of Γ modulo $F_n(x_n), \ldots, F_1(x_1)$

Theorem: $p_1 \in k$ iff $\gamma \in k$ and $p_1 = \gamma$.

We can test if γ is invariant by G and compute its value in k.
Problem 1 is solved !... when F_i are computed ...

Example

(i14) factor(x^6+2); (o14) x^6+2
Then $F_1 = x_1^6 + 2$, α_1 a root of F_1.

Factorize f over $k(\alpha_1) \equiv k[x_1]/ < f(x_1) >$
(i16) factor($x^6+2, x1^6+2$);
(o16) $(x - x1) * (x + x1) * (x^2 - x * x1 + x1^2) * (x^2 + x * x1 + x1^2)$
We can choose $F_2 = x_2 + x_1$ and $F_3 = x_3^2 - x_3 x_1 + x_1^2$
- $\alpha_2 = -\alpha_1$ the root of $f_2 = x + \alpha_1 = x - \alpha_2$
- α_3 a root of $f_3 = x^2 - \alpha_1 x + \alpha_1^2 = (x - \alpha_3)(x - \alpha_4)$
Then $F_4 = x_4 + x_3 - x_1$ and $k(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = k(\alpha_1, \alpha_3)$.
$x^2 + x\alpha_1 + \alpha_1^2 = (x - \alpha_3 + \alpha_1)(x + \alpha_3)$ over $k(\alpha_1, \alpha_3)$
(computable in Sage or Magma)
Then $F_5 = x_5 + x_1 - x_3$ and $F_6 = x_6 + x_3$

The last extension has degree $\mid G \mid = dim_k k(\underline{\alpha})$
Problem 4 Compute efficiently (without factorize on big extensions).

Compute with fundamental moduli

$f = x^6 + 2$

Fundamental moduli
$F_1 = x_1^6 + 2, F_2 = x_2 + x_1, F_3 = x_3^2 - x_3x_1 + x_1^2$
$F_4 = x_4 + x_3 - x_1, F_5 = x_5 + x_1 - x_3, F_6 = x_6 + x_3$

Roots : $\alpha_1, \ldots, \alpha_n$ s.t. $F(\underline{\alpha}) = 0$ (not any order !!!).

Solvablity Yes! $\alpha_1 = \sqrt[6]{2}$
degrees 1,2,1,1,1 of f_i are < 6:
$\alpha_2 = -\alpha_1$, $2\alpha_3 = \alpha_1 - i\sqrt{3}\alpha_1 = -2\alpha_6$, $\alpha_4 = \alpha_1 - \alpha_3 = -\alpha_5$

Normal form p_1 of Γ: $deg_{x_i}(p_1) < deg_{x_i}(F_i)$ and $\Gamma(\underline{\alpha}) = p_1(\underline{\alpha})$.

Examples:
- $\gamma = \alpha_1 + \alpha_3$; $\Gamma = p_1 = x_1 + x_3 \Rightarrow \gamma$ not invariant by G, $\gamma \notin k$.
- $\gamma = \alpha_2^2 + \alpha_1$

$$\Gamma = p_6 = \cdots = p_3 = x_2^2 + x_1 = (x_2 - x_1)F_2 + x_1^2 + x_1$$

Then $p_2 = p_1 = x_1^2 + x_1 \notin k$. Thus $\gamma \notin k$.

The Galois group ; point of view of Vandermonde, 1771

$f = x^6 + 2$

Fundamental moduli

$F_1 = x_1^6 + 2, F_2 = x_2 + x_1, F_3 = x_3^2 - x_3 x_1 + x_1^2$

$F_4 = x_4 + x_3 - x_1, F_5 = x_5 + x_1 - x_3, F_6 = x_6 + x_3$

The Galois group G of $\underline{\alpha}$ makes sens: the set of permutations σ s.t.

$$F_i(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0 \qquad i = 1, \ldots, n$$

$\mid G \mid = deg_{x_1}(F_1) \cdots deg_{x_n}(F_n) = 12$ and G transitive

=> G is a conjugate of D_6 or of $A_4(6)^+$. With F_i we obtain

$$G =< \sigma = (1,3)(2,6)(4,5), (1,2,4)(3,6,5), (2,4)(5,6) >$$

Note Easy to compute F_5, F_6 from F_2 and F_4 without factorisations:

$$F_5 = \sigma.F_4 \quad F_6 = \sigma.F_2$$

=> Systematic deductions from informations on G

The ideal of $\underline{\alpha}$-relations

$\gamma = \Gamma(\underline{\alpha}) = p_1(\underline{\alpha})$ where p_1 is the normal form of Γ
$p_1 \in k$ iff $\Gamma - p_1$ is an $\underline{\alpha}$-relation : $\Gamma(\underline{\alpha}) - p_1 = \gamma - p_1 = 0$

Let $\mathfrak{M}$ the set (maximal ideal) of $\underline{\alpha}$-relations : $r(\alpha_1, \ldots, \alpha_n) = 0$.

Definition: The Galois group of $\underline{\alpha}$ (not f!) is the Stabilisator of the ideal $\mathfrak{M}$

$$G = \{\sigma \in S_n \mid r(\alpha) = 0 => \sigma.r(\underline{\alpha}) = 0\}$$

Theorem: The fundamental moduli form a separable triangular basis of $\mathfrak{M}$ (a Gröbner basis).
Theorem (Aubry-AV, 1998): *The initial degrees of F_i are respectively the cardinality of some subgroups of G.*
If G is known => Compute the initial degree by Theorem 3.
If F_i are known => Compute G (Theorems 1 and 3).

- $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$
- $L \subset S_n$, not necessary a group.

Galoisian ideal of $\underline{\alpha}$ defined by L:

$$I^L = \{P \in k[x_1, \ldots, x_n] \mid \sigma.P(\underline{\alpha}) = 0\}$$

Theorem GL is the stabilizer of I^L and Zero(I^L)=$GL.\underline{\alpha}$

as $I^{GL} = I^L$ we can suppose $L = GL$

Theorem Γ invariant by L => the reduction p_1 of Γ modulo I^L belongs to k and $\gamma = p_1$.

It not necessary to known $\mathfrak{M}$ to compute the value of γ in k.

Theorem (Aubry-AV, 1998) If L is a group containing G then I^L is generated by a separable triangular ideal.

- Symmetric relations ideal: $\mathcal{S} = I^{S_n}$
- $\underline{\alpha}$-relation ideal: $\mathfrak{M} = I^{I_n} = I^L = I^G$ for each subset L of G.
- $$\mathcal{S} \subset I^L \subset \mathfrak{M}$$
  with $Stab(\mathfrak{M}) = G \subset Stab(I^L) \subset Stab(\mathcal{S}) = S_n$
- if
  $$\mathcal{S} \subset I \subset \mathfrak{M}$$
  then I galoisian ideal with $S_n \subset Stab(I^L) \subset G$.

- Symmetric relations ideal: $\mathcal{S} = I^{S_n}$
- $\underline{\alpha}$-relation ideal: $\mathfrak{M} = I^{I_n} = I^L = I^G$ for each subset L of G.
- $$\mathcal{S} \subset I^L \subset \mathfrak{M}$$
  with $Stab(\mathfrak{M}) = G \subset Stab(I^L) \subset Stab(\mathcal{S}) = S_n$
- if
  $$\mathcal{S} \subset I \subset \mathfrak{M}$$
  then I galoisian ideal with $S_n \subset Stab(I^L) \subset G$.

Galoisian correspondence on galoisian ideals

- Symmetric relations ideal: $\mathcal{S} = I^{S_n}$
- $\underline{\alpha}$-relation ideal: $\mathfrak{M} = I^{I_n} = I^L = I^G$ for each subset L of G.
- $$\mathcal{S} \subset I^L \subset \mathfrak{M}$$

  with $Stab(\mathfrak{M}) = G \subset Stab(I^L) \subset Stab(\mathcal{S}) = S_n$
- if

  $$\mathcal{S} \subset I \subset \mathfrak{M}$$

  then I galoisian ideal with $S_n \subset Stab(I^L) \subset G$.

- Symmetric relations ideal: $\mathcal{S} = I^{S_n}$
- $\underline{\alpha}$-relation ideal: $\mathfrak{M} = I^{I_n} = I^L = I^G$ for each subset L of G.
- $$\mathcal{S} \subset I^L \subset \mathfrak{M}$$
  with $Stab(\mathfrak{M}) = G \subset Stab(I^L) \subset Stab(\mathcal{S}) = S_n$
- if
  $$\mathcal{S} \subset I \subset \mathfrak{M}$$
  then I galoisian ideal with $S_n \subset Stab(I^L) \subset G$.

Compute relative resolvents

Put $I := I^L$

I-Relative resolvent: $R_{\Theta,I} = R_{\Theta,L}$ already defined when L is a group containing G.

Coefficients of $R_{\Theta,I}$ invariant by G => belong to k.

- Aubry-AVB: by elimination (1998, 2009) and by multi-modular computation (2010) when I triangular

- Abdeljaouad-Bouazizi-AVB: by effectiveness of Galois Theorem (2010), by algebraic certification of the numerical method (2010).

=> Problem 3 solved=> efficient determination of G with algebraic method (see GaloisianIdeal Algo) we have

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

where $h = \mid H \mid$ and $\chi_{\Theta,I}$ is the characteristic polynomial of the mutiplicative endomorphism of $k[x_1, \ldots, x_n]/I$ induced by Θ
=> $R_{\Theta,I} \in k[x]$ (k perfect field), by linear albebra without use the Galois group

=> When $I = \mathfrak{M}$ and $R_{\Theta,I}$ is the Galois resolvent, we can prove easely Galois theorems.

As $k(\alpha_1, \ldots, \alpha_n)$ isomorphic to $k[x_1; \ldots, x_n]/\mathfrak{M}$ and $\sqrt{\mathfrak{M}} = \mathfrak{M}$ (galoisian ideal are radical),

we have this classical result: $\mid G \mid = [k(\underline{\alpha}) : k]$
Actually

$$\mid G \mid = \mid Zero(\mathfrak{M}) \mid = dim_k(k[x_1; \ldots, x_n]/\mathfrak{M}) = [k(\underline{\alpha}) : k]$$

=> Galois theory can be view as linear algebra

GaloisianIdeal Algorithm, AV

Compute $\mathfrak{M}$ from $\mathcal{S}$:
Construct a chain of galoisian ideals:

$$\mathcal{S} \subset I_1 \subset I_2 \cdots \subset \mathfrak{M}$$

with **Primitive element Theorem**(AV, 1995) on galoisian ideals:

$$I_{i+1} = I_i + < h(\Theta) >$$

where $h(x)$ is a factor of a some relative resolvent R_{Θ, I_i} of $\underline{\alpha}$ computed with I_i as explained before

The relative resolvent R_Θ excludes groups as Galois group (groups matrices, AV, 1995)

Resolvents are usefull to compute generators of galoisian ideals and find Galois groups.

=> $\mathfrak{M}$ and G are computed simultaneously

Other similar work: Ducos and Quitté, 2000

Other methods to compute $\mathfrak{M}$

- Multivariate Interpolation (Burberger-Möller algorithm for Gröbner basis): Lederer, 2004 (G is known), McKay-Stauduhar, 1996 (linear relations only)
- Linear method: Yokoyama, 1999
- p-adic method : Yokoyama, 1994
- Mixed method with pre-computation of F_i from permutations and euclidean division (very efficient): Orange-Renault-AV, 2003; AV, 2008.
- Dynamic methods: Lombardi and Diaz-Toca, 2009

. . . ...

See manuscrit of Toni Machi on the Web

Conclusion:

Mixe all the methods in a parallel and collaborative computation is the better method

Thanks Toni!

Toni

J'ai pu travailler fructueusement à partir de documents précieux que tu m'as fait découvrir. Merci pour ta collaboration et ta bienveillance depuis plus de 20 ans.