Galois ideals and groups

Annick Valibouze

Laboratoires LSTA et LIP6
Université Paris 6
France

Let

$$f(x) = x^3 + 1,$$

with the roots :

$\alpha_1 = exp(i\frac{\pi}{3}),\ \alpha_2 = exp(i\pi) = -1,\ \alpha_3 = exp(i\frac{5\pi}{3}).$

One has :

$$\alpha_1^3 - \alpha_2 = exp(i\frac{\pi}{3})^3 + 1 = 0,$$

i.e the *relation* :

$$r = x_1^3 - x_2.$$

Consider the permutation $\sigma = (1)(2,3)$. Then

$$\sigma.r = x_1^3 - x_3, \text{ and } \alpha_1^3 - \alpha_3 \neq 0.$$

Therefore if $\beta = \alpha_1^3 = \alpha_2$ how can one define the action of σ on β ?

Either $\sigma(\beta) = \sigma(\alpha_1^3) = \alpha_{\sigma(1)}^3 = \alpha_1^3$;

or $\sigma(\beta) = \sigma(\alpha_2) = \alpha_{\sigma(2)} = \alpha_3$.

However, $\alpha_1^3 \neq \alpha_3$.

Instead of r, let us now choose special relations. From :

$$\begin{aligned} f(x) &= x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 \\ &\quad +(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x \\ &\quad -\alpha_1\alpha_2\alpha_3 \\ &= x^3 - 0 \cdot x^2 + 0 \cdot x + 1, \end{aligned}$$

we have the *symmetric relations among the roots of* f :

$$\begin{aligned} r_1 &= x_1 + x_2 + x_3 - 0, \\ r_2 &= x_1x_2 + x_1x_3 + x_2x_3 - 0, \\ r_3 &= x_1x_2x_3 + 1. \end{aligned}$$

They generate the ideal of symmetric relations

$$\mathcal{S} = \langle r_1, r_2, r_3 \rangle$$

in $\mathbf{Q}[x_1, x_2, x_3]$.

One can prove that :

$$S = \{r \in \mathbf{Q}[x_1, x_2, x_3] \mid \sigma.r(\alpha_1, \alpha_2, \alpha_3) = 0,\ \forall \sigma \in S_3\}$$

For the other relations (non symmetric ones), consider the ideal :

$$\mathcal{M} = \{r \in Q[x_1, x_2, x_3] \mid r(\alpha_1, \alpha_2, \alpha_3) = 0\}$$

Look for :

$$G = \{\tau \in S_3 \mid \tau.r \in \mathcal{M}, \forall r \in \mathcal{M}\}$$

(i.e. if r is a relation, $\tau.r$ also is a relation).

We already know that $\sigma = (1)(2,3) \notin G$.

G is a group, the Galois group of the triple $\underline{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$.

With a different order of the roots, e.g.

$$\underline{\beta} = \sigma.\underline{\alpha} = (\alpha_1, \alpha_3, \alpha_2)$$

we have the conjugate $\sigma^{-1}G\sigma$.

We define the zeros $\mathcal{Z}(I)$ of an ideal I as the set of triples on which all the elements of I vanish. We have

$$\mathcal{Z}(\mathcal{S}) = \{\sigma.\underline{\alpha}, \mid \sigma \in S_n\} = S_n.\underline{\alpha}.$$

Therefore

$$\mathcal{Z}(\mathcal{M}) = \{\sigma.\underline{\alpha}, \mid \sigma \in G\} = G.\underline{\alpha}.$$

Let $Id(E)$ be the ideal of polynomials with coefficients in Q vanishing in E. Clearly :

$$\mathcal{S} = Id(S_n.\underline{\alpha}),$$

$$\mathcal{M} = Id(\{\underline{\alpha}\}) = Id(G.\underline{\alpha}).$$

Since $G \subseteq S_n$ we have :

$$\mathcal{S} \subseteq \mathcal{M}.$$

If $\mathcal{M}$ is known, G is also known.

Let be the surjective morphism

$$\begin{array}{rccc} \psi: & \mathbf{Q}[\underline{x}] & \longrightarrow & Q(\underline{\alpha}) \\ & p(\underline{x}) & \mapsto & p(\underline{\alpha}) \end{array} .$$

Its kernel is $\ker(\psi) = \mathcal{M}$.

$$\mathbf{Q}[\underline{x}]/\mathcal{M} \simeq Q(\underline{\alpha})$$

a field. Thus $\mathcal{M}$ is a maximal ideal.

To calculate $\mathcal{M}$

We know that

$$r = x_1^3 - x_2 \notin \mathcal{S}$$

(otherwise $\sigma.r = x_1^3 - x_3 \in \mathcal{S} \subseteq \mathcal{M}$) and that

$$r \in \mathcal{M},$$

because $\alpha_1^3 - \alpha_2 = 0$.

Therefore, $G \neq S_3$.

Actually, $f(x) = (x+1)(x^2 - x + 1)$.

The roots satisfy the following relations :

$$\begin{aligned} \alpha_1^2 - \alpha_1 + 1 &= 0, \\ \alpha_2 + 1 &= 0, \\ \alpha_3 + \alpha_1 - 1 &= 0. \end{aligned}$$

Therefore, the polynomials

$f_1 = x_1^2 - x_1 + 1, f_2 = x_2 + 1, f_3 = x_3 + x_1 - 1$

belong to $\mathcal{M}$.

If the ideal I generated by f_1, f_2, f_3 is smaller than $\mathcal{M}$, then

$$\mathcal{Z}(I) = \{(\alpha_1, \alpha_2, \alpha_3), (\alpha_3, \alpha_2, \alpha_1)\} \supset \mathcal{Z}(\mathcal{M})$$

and the system of equations obtained by setting equal to zero the generators of $\mathcal{M}$ has only one solution $(\alpha_1, \alpha_2, \alpha_3)$. We have

$$\mathcal{Z}(\mathcal{M}) = \{(\alpha_1, \alpha_2, \alpha_3)\} = G.\underline{\alpha}$$

Then G is the identity group and

$$x_1 - \alpha_1, x_2 - \alpha_2, x_3 - \alpha_3 \in \mathcal{M}.$$

It is impossible because $\alpha_1 \notin \mathbf{Q}$. Then

$$\mathcal{M} = I \quad .$$

$$G = \{id, (1,3)\},$$

$$\mathcal{Z}(\mathcal{M}) = \{(\alpha_1, \alpha_2, \alpha_3), (\alpha_3, \alpha_2, \alpha_1)\},$$

$$S_3 = G + G(1,2) + G(2,3),$$

We have two other maximal ideals including S_3 :

$$(1.2).\mathcal{M} = \langle x_1{+}1, x_2^2{-}x_2{+}1, x_3{+}x_1{-}1\rangle, \ \{id, (2,3)\},$$

$$(2,3).\mathcal{M} = \langle x_1^2{-}x_1{+}1, x_2{+}x_1{-}1, x_3{+}1\rangle, \ \{id, (1,2)\}.$$

The ideal of symmetric relations is the intersection of 3 maximal ideals :

$$\mathcal{S} = \mathcal{M} \cap (1.2).\mathcal{M} \cap (2,3).\mathcal{M}$$

$$\mathcal{Z}(\mathcal{S}) = \mathcal{Z}(\mathcal{M}) \cup \mathcal{Z}((1.2).\mathcal{M}) \cup \mathcal{Z}((2,3).\mathcal{M}).$$

Remark

The elements of G, id and $\tau = (1,3)$, yield the field automorphisms :

$$\mathbf{Q}(\alpha_1, \alpha_2, \alpha_3) \longrightarrow \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3)$$

induced by $\alpha_i \to \alpha_i$ and $\alpha_i \to \alpha_{\tau(i)}$.

The general case

Dramatis personae :

k a perfect field,

$f(x) = \prod_{i=1}^{n}(x - \alpha_i) \in k[x]$,

$\underline{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \bar{k}$

the ideal of symmetric relations generated by the triangular system formed by the Cauchy moduli of f :

$$\begin{aligned} \mathcal{S} &= \{p \in k[\underline{x}] \mid \forall \sigma \in S_n,\ p(\sigma.\underline{\alpha}) = 0\}; \\ &= Id(S_n.\underline{\alpha}) \end{aligned}$$

the ideal of $\underline{\alpha}-$relations :

$$\mathcal{M} = Id(\{\underline{\alpha}\}) = Id(G.\underline{\alpha});$$

the Galois group of $\underline{\alpha}$ over k :

$$G = \{\sigma \in S_n \mid \sigma.\mathcal{M} = \mathcal{M}\}$$

$$\mathcal{Z}(\mathcal{S}) = S_n.\underline{\alpha} \quad \supseteq \quad \mathcal{Z}(\mathcal{M}) = G.\underline{\alpha}$$

$$S_n = G\tau_1 + G\tau_2 + \cdots + G\tau_s$$

$$\mathcal{S} = \mathcal{M}_1 \cap \mathcal{M}_2 \ldots \cap \mathcal{M}_s$$

where $\mathcal{M}_i = \tau_i^{-1}.\mathcal{M}$ is the ideal of the $\tau_i.\underline{\alpha}-$relations.

Problem

$\mathcal{S}$ is known

How to determine $\mathcal{M}$, i.e. how to find a triangular system of polynomials that generate $\mathcal{M}$?

$$k(\underline{\alpha}) \simeq k[\underline{x}]/\mathcal{M}$$

We have :

$$|G| = |\mathcal{Z}(\mathcal{M})| = dim_k(k[\underline{x}]/\mathcal{M})$$

(since $\mathcal{M}$ is a radical ideal).

Various methods for determining $\mathcal{M}$

1st method Galois resolvent

This makes use of a polynomial :

$$V(x_1, \ldots, x_n) = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n,\ \lambda_i \in k$$

only invariant under the identity and s.t. the *(absolute) resolvent* of f by V :

$$R_V(x) = \prod_{\sigma \in S_n} (x - V(\sigma.\underline{\alpha}))$$

only has distinct roots.

Let $v = V(\underline{\alpha}) \in k(\underline{\alpha})$. Then :

$$Min_v(x) \text{ is a factor of } R_V(x)$$

and

$$Min_v(V) \text{ belongs to } \mathcal{M}$$

since $M_v(V(\underline{\alpha})) = 0$.

Thus, by definition of G, one can show that

$$Min_v(x) = \prod_{\sigma \in G} (x - V(\sigma.\underline{\alpha})).$$

We have :

$i)$ $deg_x(Min_v(x)) = |G| = dim_k(k(\underline{\alpha}))$,

so that v is a primitive element of $k(\underline{\alpha})$;

$ii)$ $\mathcal{M} = \mathcal{S} + \langle Min_k(V) \rangle$

The difficulties of this method are :

1. the degree of the Galois resolvent $R_V(x)$ is $n!$;

2. find a triangular system that generates $\mathcal{M}$ starting from one of $\mathcal{S}$ and $Min_k(V)$.

2d method : G-resolvent

This makes use of a polynomial only invariant under G :

$$\Theta \in k[\underline{x}]$$

and s.t. the resolvent of f by θ :

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

only has distinct roots. Then :

$a)$ $\theta = \Theta(\underline{\alpha}) \in k$;

$b)$ $\mathcal{M} = \mathcal{S} + \langle \Theta(\underline{x}) - \theta \rangle$

To prove $\theta \in k$, set $v_i = V(\sigma_i.\underline{\alpha})$, $\sigma_i \in G$, $i = 1, 2, \ldots, m$, $m = |G|$.

As v_1 is a primitive element of $k(\underline{\alpha})$ (like all v_i's),

$\theta = \Theta(\underline{\alpha}) = v_1^{m-1} + c_{m-1} v_1^{m-2} + \cdots + c_0 = p(v_1)$

with $c_i \in k$, and since $\sigma_i.\Theta = \Theta$, by definition of G, we have :

$$\theta = v_i^{m-1} + c_{m-1} v_i^{m-2} + \cdots + c_0 = p(v_i)$$

$i = 1, 2, \ldots, m$.

Thus $v_1, \ldots, v_m$ are m distinct roots of the polynomial $p(x) - \theta$ of degree $m - 1$. Il follows $p(x) \equiv 0$, so that :

$$\theta = c_0 \in k.$$

The difficulties of this method :

1. if $|G|$ is small, the degree of the resolvent $[S_n : G]$ is still high, and it is difficult to determine $\mathcal{M}$;

2. G is not necessarily known.

3d method : Factorization in extensions

(Tchebotarev–Yokoyama)

To simplify f is supposed to be irreducible.

Set $f_1(x) = f(x)$ and $f_1 = f(x_1)$.

Let us consider the field tower :

$$k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\underline{\alpha})$$

First, factoring $f_1(x)$ in

$$k(\alpha_1) \simeq k[x_1]/\langle f_1 \rangle,$$

we obtain a polynomial $f_2(x_1, x)$.

Set $f_2 = f_2(x_1, x_2)$. Factoring $f_2(x_2, x)$ in

$$k(\alpha_1, \alpha_2) \simeq k[x_1, x_2]/\langle f_1, f_2 \rangle$$

we obtain a polynomial $f_3(x_1, x_2, x)$ and so on. In the end we obtain n polynomials

$$f_1, f_2, \ldots, f_i(x_1, \ldots, x_i), \ldots, f_n(x_1, \ldots, x_n)$$

forming a triangular system of generators of $\mathcal{M}$.

Difficulties of this method.

The more the order of the Galois group is big, the more the factorizations are difficult. In fact, the product of the degrees of the polynomials f_i equals the order of the group.

4th method

Galois ideals

The idea is to split the problem by constructing a chain of ideals :

$$\mathcal{S} = I_1 \subset I_2 \subset \ldots \subset \mathcal{M}$$

such that

$$\mathcal{Z}(\mathcal{M}) \subseteq \mathcal{Z}(I) \subseteq \mathcal{Z}(S) = S_n.\underline{\alpha}$$

for all the ideals I of the chain.

Then :

$$\mathcal{Z}(I) = L.\underline{\alpha}$$

where $G \subseteq L \subseteq S_n$.

By definition, $I = Id(L.\underline{\alpha})$ is a Galois ideal

Problem :

Given I, find a Galois ideal J such that $I \subset J$.

For the sake of simplicity, let us assume that L is a subgroup of S_n.

Let $H < L$ and let $\Psi \in k[x_1, \ldots, x_n]$ only invariant under the elements of H, and s.t. the resolvent

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

has distinct roots.

$R_\Psi(x)$ belongs to $k[x]$ because $G \subset L$.

Remark

In order to determine $R_\Psi(x)$ one cannot use the fundamental theorem of symmetric functions (i.e. the ideal $\mathcal{S}$) any longer, but a triangular system of generators of I (Aubry-Valibouze, 1999).

Let $h(x)$ be a factor of $R_\Psi(x)$. We construct a new ideal :

$$J = I + \langle h(\Psi) \rangle$$

which contains I.

Now consider the orbits of the action of G on the left cosets of H in L. One of these orbits O is s.t.

$$h(x) = \prod_{\sigma | \sigma H \in O} (x - \Psi(\sigma.\underline{\alpha}))$$

and the Galois group of h is given by the left action of G on O .

We have this result for each factor of the resolvent. Then, the degrees and Galois groups of the factors of R_Ψ depend only on G and on the testing group H.

We construct two matrices $\mathcal{P}$ (Arnaudiès-Valibouze, 1974) and $\mathcal{G}$ indexed by the subgroups of L in rows and columns s.t. the element of the line of H and column of G contains :

- for $\mathcal{P}$: the cardinality of the orbits ;
- for $\mathcal{G}$: the groups given by the action of G on the orbits.

The Galois group G can be determined only using the degrees of the factors of the resolvents because the columns of the partition matrix $\mathcal{P}$ are distinct.

Submatrix $\mathcal{P}_1$ of $\mathcal{P}$ for $L = S_4$ and transitive groups only :

	S_4	A_4	D_4	C_4	V_4
A_4	2	1^2	2	2	1^2
D_4	3	3	$1, 2$	$1, 2$	1^3
C_4	6	6	$2, 4$	$1^2, 4$	2^3
V_4	6	3^2	2^3	2^3	1^6

Invariants and degrees of the resolvents :

H	R_Ψ	Invariant Ψ
S_4	1	1
A_4	2	$\prod_{i<j}(x_i - x_j)$
D_4	3	$x_1x_2 + x_3x_4$
C_4	6	$c_4 = x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2$
V_4	6	$(x_1 - x_2)(x_3 - x_4)$

Submatrix $\mathcal{P}_2$ of $\mathcal{P}$ for $L = D_4$:

	D_4	C_4
C_4	2	1^2

Let $f = x^4 + ax^3 + bx + c \in \mathbf{Q}[x]$ supposed irreducible.

$I_1 := \mathcal{S}$
The Galois group G of f is transitive in S_4.
$C := \{S_4, A_4, D_4, C_4, V_4\}$ s.t. $G \in C$.
$H := A_4$ and $R_\Psi = x^2 - disc(f)$.
Assume $d := disc(f)$ is not a square.
Then (see $\mathcal{P}_1$) $C := \{S_4, D_4, C_4\}$ and
$I_1 + \langle \Psi^2 - d \rangle = I_1$
$H := D_4$ and R_Ψ is the dihedral resolvent.
Assume $x - \psi$ is a simple factor of R_Ψ.
Then $C := \{D_4, C_4\}$ and $I_2 := I_1 + \langle \Psi - \psi \rangle$.
$H := C_4$, $D_4 = C_4 + C_4\tau$ and
$R_\Psi = (x - c_4(\underline{\alpha}))(x - c_4(\tau.\underline{\alpha}))$.
Suppose that $\psi \in \mathbf{Q}$ is a simple root.
Then (see $\mathcal{P}_2$) :

$$\mathcal{M} := I_2 + < \Psi - \psi > \text{ and } G := C_4.$$

Factorisations in extensions : the first steps are easy :

The ideal $\mathcal{M}$ of the previous example is computable with only one factorization in $\mathbf{Q}(\alpha_1)$:

$f = (x-\alpha_1)(x+g_2(\alpha_1))(x+g_3(\alpha_1))(x+g_4(\alpha_1))$.

Then

$\mathcal{M} := \langle f(x_1), x_2+g_2(x_1), x_3+g_3(x_1), x_4+g_4(x_1)\rangle$.

Therefore this method is nice for small groups.

When using Galois ideals, the last steps are easy because the degrees of the initial monomials of generating triangular systems decrease.

How can one mix these methods ? (initial work : Orange, Renault, Valibouze, 2003)

Step 1 Factorize f in $k(\alpha_1)$.

Step 2 Check the **split table** : the submatrix of groups and partitions for $H = S_1 \times S_{n-1}$ and $Stab(G, 1) = G_{\{1\}}$ possible Galois groups of f over $\mathbf{Q}(\alpha_1)$ to get rid of possible Galois groups G.

Split table in degree 4 for transitive groups G.

Deg	$G_{\{1\}}$	G	init Degree of $\mathcal{M}$
1^4	S_1^4	$V_4^+ \ C_4$	$[4, 1^3]$
$1^2, 2$	S_1^2 , S_2	D_4	$[4, 2, 1^2]$
$1, 3$	S_1 , A_3	A_4^+	$[4, 3, 1^2]$
$1, 3$	S_1 , S_3	S_4	$[4, 3, 2, 1]$

Step 3 Compute a Galois ideal I by using the Cauchy moduli of factors of f in $\mathbf{Q}(\alpha_1)$ and use the split table to compute the set L s.t. $\mathcal{Z}(I) = L.\underline{\alpha}$.

For example, let :

$$f = (x - \alpha_1)(x + g(\alpha_1))(x^2 + u(\alpha_1)x + v(\alpha_1)).$$

Then $G = D_4$ and

$$\begin{aligned}\mathcal{M} \;=\; & \langle f(x_1), x_2 + g(x_1), \\ & x_3^2 + u(x_1)x_3 + v(x_1), x_4 + x_3 + u(x_1)\rangle.\end{aligned}$$

Step 4 Compute $J = \{\sigma.I \mid \sigma \in H\}$ for H the bigger group included in L and containing G. We have $I \subset J$ with $I = J$ iff $L = H$. This step can be treated by pre-computations.

Step 5 Compute $\mathcal{M}$ by using the Galois ideal method with $I_1 := J$ or continue to factorize polynomials of J in extensions.

Note : If I is any Galois Ideal with $\mathcal{Z}(I) = L.\underline{\alpha}$ then $I \subset J = L.I$ with $I = J$ iff L is a group and $\mathcal{Z}(J) = H.\underline{\alpha}$ where H is a group (S. Orange, 2003).

Comments : The previous algorithm can be pre-constructed. Then the polynomials that we must compute (not with Cauchy moduli and not in Step 4) can be knowed by advance if the Galois group is knowed or partially knowed. In that case this *principal* polynomials can be computed by any method as the p-adic of K. Yokoyama which computes directly $\mathcal{M}$ by using its initial degree (private communication, 1999). This work has been realized by G. Renault and K. Yokoyama (2004).

A book is being written on this material, a joint work of Prof. Machì and myself. We expect the book to be published before the Gulf Stream ends its trip towards the North. This fact, together with the beauty of Rome, partly explains my visit to Italy.

This talk also includes some joint work with Jean-Marie Arnaudiès, Philippe Aubry and my PhD students Guenaël Renault and Sebastien Orange.