# Classes Doubles, Idéaux de Galois et Résolvantes

Annick Valibouze

# CLASSES DOUBLES, IDÉAUX DE GALOIS ET RÉSOLVANTES

ANNICK VALIBOUZE

Results on permutation groups are applied to Galois theory.

*AMS 2000 Subject Classification:* 12F10, 12Y05, 11Y40.

*Key words:* Galois group, Galois ideal, triangular ideal, splitting field.

## 1. INTRODUCTION

Les classes doubles, un outil classique de la théorie des groupes (voir Paragraphe 4), trouvent des applications en la théorie de Galois effective. Nous montrons comment elles interviennent

- sur les idéaux de Galois (définis au Paragraphe 2) pour obtenir des informations sur les injecteurs (voir Paragraphe 5) et
- sur les résolvantes (définies au Paragraphe 3) pour obtenir des informations sur leurs facteurs irréductibles (voir Paragraphe 6).

Nous terminerons par un exemple d'application (voir Paragraphe 7).

Dans tout cet article, nous nous donnons un polynôme $f$ d'une variable sur un corps parfait $k$. Nous le supposons séparable de degré $n$ et nous notons $\underline{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ un $n$-uplet formé par les $n$ racines distinctes de $f$ (dans une clôture algébrique de $k$).

Nous notons $S_n$ le groupe symétrique de degré $n$ et fixons $x_1, \ldots, x_n$, $n$ variables algébriquement indépendantes sur $k$. Le groupe $S_n$ agit naturellement sur l'anneau de polynômes $k[x_1, \ldots, x_n]$ : pour $\sigma \in S_n$ et $p \in k[x_1, \ldots, x_n]$, $\sigma.p = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Pour $E \subset k[x_1, \ldots, x_n]$, nous posons $\sigma.E = \{\sigma.p \mid p \in E\}$. Pour $H \subset S_n$, nous posons $H.p = \{\sigma.p \mid \sigma \in H\}$ et $H.E = \{\sigma.E \mid \sigma \in H\}$.

Les sous-groupes transitifs de $S_8$ notés $8T_i$ correspondent aux groupes tabulés dans le logiciel Magma et respectivement obtenus par l'appel `TransitiveGroup(8,i)` (voir [5]).

## 2. IDÉAUX DE GALOIS

Les idéaux de Galois ont été introduits dans [11]. Les résultats énoncés et non démontrés proviennent de cet article que nous ne citons pas systématiquement; nonobstant, la terminologie *stabilisateur* est généralisée ici par la terminologie *injecteur*.

L'idéal

$$\mathfrak{M} = \{r \in k[x_1, \ldots, x_n] \mid r(\alpha_1, \ldots, \alpha_n) = 0\}$$

est un idéal maximal dans $k[x_1, \ldots, x_n]$ car noyau du morphisme surjectif d'évaluation entre l'anneau $k[x_1, \ldots, x_n]$ et le corps de décomposition $K = k(\alpha_1, \ldots, \alpha_n)$ de $f$. Cet idéal est appelé l'*idéal des $\underline{\alpha}$-relations*. Il est engendré par un ensemble triangulaire de polynômes

$$r_1(x_1), r_2(x_1, x_2), \ldots, r_7(x_1, \ldots, x_n)$$

où chaque polynôme $r_i$ est unitaire de degré $d_i$ en $x_i$ (voir [10]). Calculer le corps $K$ revient à obtenir un tel ensemble triangulaire. Les degrés $d_1, d_2, \ldots, d_n$ sont appelés les *degrés initiaux* de l'ensemble triangulaire ou de l'idéal. Cette définition est étendue à tout idéal engendré par un ensemble triangulaire.

**Note.** Rappelons une propriété classique. Pour que la rédaction d'un polynôme modulo $\mathfrak{M}$ soit nulle si et seulement si il appartient à $\mathfrak{M}$, il faut et il suffit que l'ensemble $r_1, \ldots, r_n$ soit réduit; c'est-à-dire que

$$r_i = x_i^{d_i} + g(x_1, \ldots, x_i)$$

avec $g \in k[x_1, \ldots, x_i]$ et $\deg_{x_j} g < d_j$ pour $j = 1, \ldots, i$. Pour y parvenir, il suffit d'opérer des divisions euclidiennes sur l'ensemble triangulaire générateur.

L'idéal

$$\mathfrak{J} = \bigcap_{\sigma \in S_n} \sigma.\mathfrak{M},$$

appelé l'*idéal des relations symétriques*, est engendré par l'ensemble triangulaire formé par les *modules de Cauchy* du polynôme $f$ (voir [9]). Auparavant, il n'était défini que par ses générateurs: les modules de Cauchy (voir [6] et [10]).

De manière générale, considérons l'idéal

$$I = \bigcap_{\sigma \in L} \sigma.\mathfrak{M}$$

où $L$ est une partie de $S_n$. Nous l'appelons l'*idéal de Galois défini par $L$ et $\mathfrak{M}$* (sur $k$). Nous dirons que $I$ est un *idéal de Galois de $f$* (sur $k$).

L'*injecteur* $\mathrm{Inj}(I, J)$ *de $I$ dans $J$*, un idéal contenant $I$, est l'ensemble des permutations de $S_n$ qui envoient $I$ dans $J$:

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

L'injecteur de $I$ dans $\mathfrak{M}$ est la plus grande partie de $S_n$ définissant l'idéal $I$ avec $\mathfrak{M}$. Pour la suite, nous supposons donc que

$$L = \mathrm{Inj}(I, \mathfrak{M}).$$

L'injecteur $\mathrm{Inj}(I, I)$ est appelé le *groupe de décomposition de* $I$. Si $\mathrm{Inj}(I, \mathfrak{M})$ est un groupe alors l'idéal $I$ est dit *pur* et cet injecteur s'identifie au groupe de décomposition de $I$. Nous avons le résultat suivant.

THÉORÈME 2.1 (voir [11] et [4]). *Un idéal de Galois est pur si et seulement s'il vérifie l'une des conditions suivantes:*

- *il est défini par un groupe et il est engendré par un ensemble triangulaire dont le produit des degrés initiaux est identique au cardinal de son groupe de décomposition;*
- *il est défini par un sur-groupe du groupe de décomposition d'un idéal maximal $\mathfrak{M}'$ qui le contient.*

Les idéaux $\mathfrak{J}$ et $\mathfrak{M}$ sont purs de groupes de décomposition respectifs $S_n$ et $\mathrm{Gal}_k(\underline{\alpha})$, *le groupe de Galois de* $\underline{\alpha}$ *sur* $k$. Le cardinal du groupe $\mathrm{Gal}_k(\underline{\alpha})$ est le produit $d_1 d_2 \cdots d_n$ des degrés initiaux de $\mathfrak{M}$ (voir le Théorème 2.1). Le groupe $\mathrm{Gal}_k(\underline{\alpha})$ est isomorphe au groupe des $k$-autormorphismes du corps de décomposition $K$ de $f$ (i.e., le groupe de Galois de $K$ sur $k$).

Ci-après, nous énonçons des résultats inhérents aux injecteurs.

PROPOSITION 2.2. *Soit $c$ l'ordre du groupe de Galois* $\mathrm{Gal}_k(\underline{\alpha})$. *Supposons que $I$ soit engendré par un ensemble triangulaire et que $m$ soit le produit des degrés initiaux de $I$. Alors* $\mathrm{Inj}(I, \mathfrak{M})$ *est de cardinal $m$ et est l'union de $m/c$ classes à droite disjointes du groupe de Galois* $\mathrm{Gal}_k(\underline{\alpha})$.

PROPOSITION 2.3. *Soient $I_1$ et $I_2$ deux idéaux de Galois de $f$ et $H \subset S_n$. Alors*

$$\mathrm{Inj}(I_1 \cup I_2, \mathfrak{M}) = \mathrm{Inj}(I_1, \mathfrak{M}) \cap \mathrm{Inj}(I_2, \mathfrak{M}) \tag{2.1}$$

*et*

$$\mathrm{Inj}(H.I, \mathfrak{M}) = \bigcap_{h \in H} \mathrm{Inj}(I, \mathfrak{M}) h^{-1}. \tag{2.2}$$

*Démonstration.* La première identité est évidente. Pour montrer la seconde, fixons $\sigma \in S_n$ et montrons que $\mathrm{Inj}(\sigma.I, \mathfrak{M}) = \mathrm{Inj}(I, \mathfrak{M})\sigma^{-1}$. Par définition de l'injecteur, il vient

$$\mathrm{Inj}(\sigma.I, \mathfrak{M}) = \{\tau \in S_n \mid \tau\sigma.I \in \mathfrak{M}\} = \{\rho \in S_n \mid \rho.I \in \mathfrak{M}\}\sigma^{-1} = \mathrm{Inj}(I, \mathfrak{M})\sigma^{-1}.$$

D'où $\mathrm{Inj}(H.I, \mathfrak{M}) = \bigcap_{h \in H} \mathrm{Inj}(h.I, \mathfrak{M}) = \bigcap_{h \in H} \mathrm{Inj}(I, \mathfrak{M}) h^{-1}$. □

Le résultat suivant découle de la Proposition 2.3.

PROPOSITION 2.4. *Soient $H$ une partie de $S_n$ et $h \in H$. Soit $J$ un idéal de Galois de $f$ sur $k$ contenu dans $\mathfrak{M}$ tel que* $\mathrm{Inj}(J, \mathfrak{M}) = H\,\mathrm{Inj}(J, \mathfrak{M})$. *Alors* $\mathrm{Inj}(J', \mathfrak{M}) = H\,\mathrm{Inj}(J', \mathfrak{M})$ *pour chaque idéal $J'$ dans $\{h.J, J + h.J, H.J\}$.*

## 3. RÉSOLVANTES

L'article historique publié par Lagrange (voir [7]) en 1770 est le premier à considérer les racines d'un polynôme (d'une équation) comme des quantités abstraites plutôt qu'ayant des valeurs numériques. Il peut être considéré comme la première étape du développement de la théorie des groupes poursuivie par Ruffini, Galois et Cauchy. C'est dans cet article que Lagrange introduit la résolvante. La résolvante est un outil essentiel pour déterminer le groupe de Galois mais aussi pour calculer des relations (voir [11]). Nous la définissons ci-après d'un point de vue plus général que celui de Lagrange.

Soit $\Theta \in k[x_1, \ldots, x_n]$. Le polynôme

$$R(\Theta, I) = \prod_{\Psi \in \mathrm{Inj}(I, \mathfrak{M}).\Theta} (x - \Psi(\alpha_1, \ldots, \alpha_n))$$

est appelé la *résolvante de $\underline{\alpha}$ par $\Theta$ relative à $I$* (ou bien à $\mathrm{Inj}(I, \mathfrak{M})$). La résolvante est une racine du polynôme caractéristique de l'endomorphisme de multiplication par $\Theta$ dans l'anneau quotient $k[x_1, \ldots, x_n]/I$. Donc, par l'algèbre linéaire et puisque le corps $k$ est parfait, la résolvante $R(\Theta, I)$ est à coefficients dans $k$.

*Notations* 3.1. Nous posons $\theta = \Theta(\alpha_1, \ldots, \alpha_n)$ et, pour $\sigma \in S_n$, nous notons $\theta^\sigma$ le polynôme $\sigma.\Theta(\alpha_1, \ldots, \alpha_n)$.

Soit $M$ un sous-groupe de $S_n$ contenant $\mathrm{Gal}_k(\underline{\alpha})$. L'idéal de Galois $I_M$ défini par $M$ et $\mathfrak{M}$ est pur de groupe de décomposition $M$ et contenu dans l'idéal $I$.

Supposons que l'injecteur $\mathrm{Inj}(I, \mathfrak{M})$ soit une partie de $M$ et fixons $H$ un sous-groupe de $M$ inclus dans $L$. Prenons $\Theta$ tel que $H$ soit le plus grand sous-groupe de $M$ vérifiant $H.\Theta = \{\Theta\}$ (i.e. $H$ est le stabilisateur de $\Theta$ dans $M$). La résolvante $R(\Theta, I)$ est un facteur (sur $k$) de la résolvante $R(\Theta, I_M)$ qui s'exprime sous la forme

$$R(\Theta, I_M) = \prod_{i=1}^{e} (x - \theta^{\sigma_i}) \tag{3.1}$$

où $\{\sigma_1 H, \ldots, \sigma_e H\}$ est l'ensemble, noté $\mathcal{C}$, des classes à gauche de $M$ modulo $H$.

## 4. CLASSES DOUBLES

Dans les prochains paragraphes, nous exhiberons des propriétés algébriques sur les résolvantes et les idéaux de Galois résultantes des intersections entre des classes à droite et des classes à gauche. Les classes doubles sont appropriées à l'étude de ces intersections.

Fixons $G$ et $H$ deux sous-groupes d'un sous-groupe $M$ de $S_n$. Soit la relation d'équivalence $\mathcal{R}_{G,H} = \mathcal{R}$ définie dans $M$ par

$$\sigma \mathcal{R} \tau \quad \text{si} \quad \sigma H \cap G\tau \neq \emptyset.$$

La classe d'équivalence de $\sigma$, notée $(G\sigma H)$, est appelée une *classe double de $M$ modulo $G$ et $H$*. La notation $(G\sigma H)$ est due au résultat connu suivant.

PROPOSITION 4.1. *Soient $\sigma, \tau \in M$. Alors $\sigma \mathcal{R} \tau$ si et seulement si $\tau \in G\sigma H$.*

## 5. IDÉAUX DE GALOIS ET CLASSES DOUBLES

Dans ce paragraphe, nous considérons les classes doubles de $S_n$ modulo $H$ et $H$, où $H$ est un sous-groupe de $S_n$.

En général, pour un sous-groupe $E$ de $S_n$, la partie $HE$ de $S_n$ n'est pas un groupe. Le résultat suivant introduit un sous-groupe de $E$ qui satisfait cette propriété.

PROPOSITION 5.1. *Soient deux sous-groupes $H$ et $E$ de $S_n$. L'ensemble*

$$\mathcal{E} = \{\sigma \in E \mid (H\sigma H) \subset HE\}$$

*est un sous-groupe de $E$ vérifiant $\mathcal{E}H = H\mathcal{E}$ et l'ensemble $H\mathcal{E}$ est un sous-groupe de $S_n$.*

*Démonstration.* Remarquons tout d'abord que $\mathcal{E} = \{\sigma \in E \mid \sigma H \subset HE\}$. L'identité appartient à $\mathcal{E}$ car elle appartient au groupe $E$ et $H \subset HE$. Montrons la stabilité de $\mathcal{E}$. Soient $\sigma, \sigma' \in \mathcal{E}$. Alors $\sigma\sigma' H \subset \sigma HE \subset HEE = HE$ car $E$ est un groupe. Donc $\mathcal{E}$ est groupe.

Montrons que $\mathcal{E}H = H\mathcal{E}$. Soit $\sigma \in \mathcal{E}$. Nous avons $\sigma H \subset HE$. Choisissons $\tau \in E$ tel que $\tau \mathcal{R} \sigma$. Comme $\mathcal{R}$ est une relation d'équivalence, $(H\tau H) = (H\sigma H) \subset H\mathcal{E}$. D'où $\tau \in \mathcal{E}$. Donc $\mathcal{E}H \subset H\mathcal{E}$. Comme $\mathcal{E}$ et $H$ sont des groupes, nous obtenons le résultat.

Montrons la stabilité de $H\mathcal{E}$ (qui contient l'identité). Comme $\mathcal{E}H = H\mathcal{E}$, nous avons $H\mathcal{E}H\mathcal{E} = HH\mathcal{E}\mathcal{E} = H\mathcal{E}$ car $H$ et $\mathcal{E}$ sont des groupes. Donc $H\mathcal{E}$ est un groupe. □

COROLLAIRE 5.2. *Sous les hypothèses de la Proposition* 5.1*, si le groupe $H$ est maximal dans $HE$ alors $H = H\mathcal{E}$ et $\mathcal{E}$ est un sous-groupe de $H$.*

*Démonstration.* Comme $H \subset H\mathcal{E} \subset HE$, si $H$ est maximal dans $EH$ alors $H = H\mathcal{E}$ puisque, d'après la Proposition 5.1, $H\mathcal{E}$ est un groupe. Le groupe $\mathcal{E}$ est donc un sous-groupe de $H$. □

Dans [8] sont construits des idéaux de Galois triangulaires d'injecteurs $HE$ où $H$ et $E$ sont deux sous-groupes de $S_n$. Soit $I$ un tel idéal. Lorsque $HE$ n'est pas un groupe, les auteurs choisissent un groupe $H$ maximal dans $HE$ et construisent un nouvel idéal de Galois $J = H'.I$ où $H'$ est inclus dans $H$. Dans leurs exemples, la plupart des idéaux $J$ sont purs. Le résultat suivant montre qu'en prenant $H' = H$ alors $J$ est un idéal de Galois pur.

THÉORÈME 5.3. *Si $H$ et $E$ sont deux sous-groupes de $S_n$ tels que*

$$\mathrm{Inj}(I, \mathfrak{M}) = HE$$

*et que $H$ est un groupe maximal dans $\mathrm{Inj}(I, \mathfrak{M})$ alors $H.I$ est un idéal de Galois pur de groupe de décomposition $H$.*

*Démonstration.* Nous avons $I \subset \mathfrak{M}$ car la partie $\mathrm{Inj}(I, \mathfrak{M}) = HE$ de $S_n$ contient l'identité. Comme $I \subset H.I$, nous avons $\mathrm{Inj}(H.I, \mathfrak{M}) \subset \mathrm{Inj}(I, \mathfrak{M})$. D'après la Proposition 2.4, $\mathrm{Inj}(H.I, \mathfrak{M}) = H\,\mathrm{Inj}(H.I, \mathfrak{M}) \subset HE$. Si $\tau \in HE$ alors $\tau = h\sigma$ avec $\sigma \in E$. La permutation $\tau$ appartient à $\mathrm{Inj}(H.I, \mathfrak{M})$ si et seulement si $\sigma$ appartient aussi à $\mathrm{Inj}(H.I, \mathfrak{M})$. Donc il suffit de considérer les permutations de $E$ appartenant à $\mathrm{Inj}(H.I, \mathfrak{M})$.

D'après la Proposition 2.3,

$$\mathrm{Inj}(H.I, \mathfrak{M}) = \bigcap_{h \in H} \mathrm{Inj}(I, \mathfrak{M})h^{-1} = \bigcap_{h \in H} HEh^{-1},$$

par hypothèse. Donc une permutation $\sigma$ de $E$ appartient à $\mathrm{Inj}(H.I, \mathfrak{M})$ si et seulement si $\sigma H \subset HE$; c'est-à-dire $\sigma \in \mathcal{E} \subset H$, d'après le Corollaire 5.2. Ainsi $H = \mathrm{Inj}(H.I, \mathfrak{M})$ et l'idéal $H.I$ est un idéal de Galois pur. □

**Note.** En 1994, suite aux travaux de [8], S. Orange a annoncé que l'idéal $\mathrm{Inj}(I, \mathfrak{M})$. $I$ est un idéal de Galois pur.

*Exemple* 5.4. Soit $f = x^8 - 3x^5 - x^4 + 3x^3 + 1$ un polynôme de groupe de Galois $G = \langle \sigma_1 = (1,3,5,8,2,7,6,4), (1,7)(2,3)(4,6)(5,8) \rangle$, un conjugué de $8T_6$ (ce polynôme est extrait de la base de donnée du logiciel Magma). Soit $I$ l'idéal de Galois de $f$ engendré par l'ensemble triangulaire formé des polynômes (exprimés dans $\mathbb{Z}[x_1, \ldots, x_7]$ afin de simplifier la présentation):

$$\begin{aligned}
r_1 &= x_1^8 - 3x_1^5 - x_1^4 + 3x_1^3 + 1,\\
r_2 &= x_2 - x_1^7 + 3x_1^4 + x_1^3 - 3x_1^2 = \mathbf{x_2} + \mathbf{h_2}(\mathbf{x_1}),\\
r_3 &= 3x_3^2 + x_3x_1^6 - x_3x_1^5 - x_3x_1^4 - 6x_3x_1^3 + x_3x_1^2 + 5x_3x_1 + 2x_3 + x_1^7 + 3x_1^6 +\\
&\quad + x_1^5 - x_1^4 - 8x_1^3 + 4x_1 - 1,
\end{aligned}$$

$$
\begin{aligned}
r_4 &= 3x_4 + 3x_3 + x_1^6 - x_1^5 - x_1^4 - 6x_1^3 + x_1^2 + 5x_1 + 2 = \mathbf{3x_4 + 3x_3 + h_3(x_1)},\\
r_5 &= 3x_5^2 + 5x_1^7x_5 - 2x_1^6x_5 + 4x_1^5x_5 - 15x_1^4x_5 + 5x_1^3x_5 +\\
&\quad + 7x_1^2x_5 - 5x_1x_5 + 3x_5 - 3,\\
r_6 &= 3x_6 + 3x_5 + 5x_1^7 - 2x_1^6 + 4x_1^5 - 15x_1^4 + 5x_1^3 + 7x_1^2 - 5x_1 + 3 =\\
&= \mathbf{3x_6 + 3x_5 + h_5(x_1)},\\
r_7 &= 3x_7^2 - 2x_1^7x_7 + x_1^6x_7 - 3x_1^5x_7 + 7x_1^4x_7 - 2x_1^3x_7 + x_1^2x_7 + 3x_1x_7 -\\
&\quad - 5x_7 + 2x_1^7 - 3x_1^6 + 2x_1^5 - 8x_1^4 + 8x_1^3 - 4x_1 + 4,\\
r_8 &= 3x_8 + 3x_7 - 2x_1^7 + x_1^6 - 3x_1^5 + 7x_1^4 - 2x_1^3 + x_1^2 + 3x_1 - 5\\
&= \mathbf{3x_8 + 3x_7 + h_7(x_1)},
\end{aligned}
$$

Construit selon la méthode de [8], cet idéal est obtenu
– en factorisant $f$ dans $\mathbb{Q}(\alpha_1)$:

$$27f = (x - \alpha_1)r_2(\alpha_1, x)r_3(\alpha_1, x)r_5(\alpha_1, x)r_7(\alpha_1, x)$$

et

– en calculant, pour $i = 3, 5, 7$,

$$r_{i+1} = (r_i(x_1, x_i) - r_i(x_1, x_{i+1}))/(x_i - x_{i+1}) = \mathbf{3x_{i+1} + 3x_i + h_i(x_1)}.$$

L'idéal $I$ vérifie les deux propriétés suivantes:

(1) il existe un idéal maximal $\mathfrak{M}$ de groupe de décomposition $G$ et contenant $I$;

(2) $\mathrm{Inj}(I, \mathfrak{M}) = GE$ où $E$ est le produit de groupes symétriques $S_1 \times S_1 \times S_2 \times S_2 \times S_2$.

Le groupe $G$ est un groupe maximal dans $GE$. Nous avons $G.I \subset \mathfrak{M}$ car $G.\mathfrak{M} = \mathfrak{M}$ et $I \subset \mathfrak{M}$. Il n'est heureusement pas nécessaire de permuter une infinité de polynômes pour calculer $G.I$; les permutés des générateurs de $I$ suffisent. Considérons les deux relations

$$\tilde{r_7} = \sigma_1.r_2 = \mathbf{x_7 + h_2(x_3)} \quad \text{et} \quad \tilde{r_5} = \sigma_1.r_4 = \mathbf{3x_5 + 3x_1 + h_3(x_3)}.$$

appartenant à $G.I$. Soit l'idéal $J$ engendré par les relations $r_1, r_2, r_3, r_4, \tilde{r_5}, r_6, \tilde{r_7}$ et $r_8$ dont le produit des degrés initiaux est identique au cardinal 16 du groupe de Galois $G$. Comme $J \subset G.I \subset \mathfrak{M}$, nous avons donc $J = \mathfrak{M} = G.I$. Le résultat $G.I = \mathfrak{M}$ est celui attendu par le Théorème 5.3.

**Note.** Il n'est pas nécessaire de calculer $r_5$ et $r_7$ pour en déduire $r_6$ et $r_8$. En effet, ils s'obtiennent en réduisant les polynômes $\sigma_1^2 \cdot r_2 = x_6 + h_2(x_5)$ et $\sigma_1^2 \cdot r_3 = 3x_8 + 3x_3 + h_3(x_5)$.

## 6. RÉSOLVANTES ET CLASSES DOUBLES

Nous reprenons les notations des Paragraphes 2, 3 et 4.

La partie $L$ de $S_n$ est supposée formée d'une union de classes à droite de $G$ dans $S_n$ et le groupe $G$ est supposé être un sous-groupe de $M$. Cette hypothèse est satisfaite lorsque $G = \mathrm{Gal}_k(\underline{\alpha})$.

Rappelons que $\mathcal{C}$ est l'ensemble des classes à gauche de $H$ dans $M$ et fixons $C_0 = \sigma H \in \mathcal{C}$. Notons $\mathcal{O}$ la $G$-orbite $\{\sigma_1 H, \sigma_2 H, \ldots, \sigma_d H\}$ de $C_0$ par action à gauche dans $\mathcal{C}$ (i.e., nous avons $GC_0 = \mathcal{O}$). Si $G = \mathrm{Gal}_k(f)$ alors, par la théorie de Galois, la résolvante $R(\Theta, I_M)$ possède un facteur $h$ sur $k$ de degré $d = \mathrm{Card}(\mathcal{O})$ s'écrivant

$$h(x) = \prod_{i=1}^{d} (x - \theta^{\sigma_i}). \tag{6.1}$$

Par la suite, lorsque nous considèrerons les polynômes, le groupe $G$ sera supposé être le groupe $\mathrm{Gal}_k(f)$.

La classe double $(G\sigma H)$ est donnée par l'union disjointe

$$(G\sigma H) = \sum_{C \in \mathcal{O}} C.$$

*Remarque* 6.1. La $G$-orbite $\mathcal{O}$ de $\sigma H$ est formée des classes à gauche $\tau H$ dans $\mathcal{C}$ telles que $\tau \in (G\sigma H)$. À chaque classe double de $M$ modulo $G$ et $H$ est associée une unique $G$-orbite d'une classe à gauche de $M$ modulo $H$; cette $G$-orbite est associée quant à elle à un unique facteur de la résolvante $R(\Theta, I_M)$.

Considérons l'ensemble

$$\mathcal{F} = \{C \in \mathcal{C} \mid C \cap L \neq \emptyset\}.$$

Nous avons

$$R(\Theta, I) = \prod (x - \theta^{\sigma_i})$$

où le produit est étendu aux $i \in [\![1, e]\!]$ tels que $\sigma_i H \in \mathcal{F}$.

La résultat suivant traduit en terme de groupes le fait suivant: si la racine $\theta^\sigma$ de $h$ est une racine de la résolvante $R(\Theta, I)$ alors les $\theta^{\sigma'}$ tels que $\sigma' H \in \mathcal{O}$ sont aussi des racines de cette résolvante; par conséquent, le polynôme $h$ est un facteur de cette résolvante que $h$ soit ou non $k$-irréductible.

Proposition 6.2. *Si $\mathcal{O} \cap \mathcal{F} \neq \emptyset$ alors $\mathcal{O} \subset \mathcal{F}$.*

*Démonstration.* Supposons que $\sigma H \in \mathcal{O} \cap \mathcal{F}$. Comme $L$ est une union de classes à droite de $G$, nous pouvons choisir $\tau \in L$ tel que $\tau \mathcal{R} \sigma$. Soit $\sigma' H$ appartenant à $\mathcal{O}$. Comme $\mathcal{O}$ est la $G$-orbite de $\sigma H$, nous avons $\sigma' \mathcal{R} \sigma$. D'où

$\tau \mathcal{R} \sigma'$, c'est-à-dire que $\sigma' H \cap G\tau \neq \emptyset$ et par conséquent $\sigma' H \cap L \neq \emptyset$. Ainsi $\sigma' H \in \mathcal{F}$. □

LEMME 6.3. *Soit* $\tau \in (G\sigma H)$ (*i.e.* $\sigma H \cap G\tau \neq \emptyset$). *Alors nous avons l'union disjointe* $G\tau = \sum_{C \subset \mathcal{O}} C \cap G\tau$.

*Démonstration.* Évident, par la définition de la $G$-orbite $\mathcal{O}$ et celle de la relation d'équivalence $\mathcal{R}$. □

LEMME 6.4. *Pour tout* $\tau, \sigma', \tau' \in S_n$ *tels que* $\sigma' \mathcal{R} \sigma$ *et* $\tau' \mathcal{R} \tau$, *nous avons l'égalité*

$$\mathrm{Card}(\sigma H \cap G\tau) = \mathrm{Card}(\sigma' H \cap G\tau').$$

*Démonstration.* Prenons $\sigma', \tau' \in S_n$ tels que $\sigma' \mathcal{R} \sigma$ et $\tau' \mathcal{R} \tau$. Si $\mathrm{Card}(\sigma H \cap G\tau) = 0$ alors, comme $\mathcal{R}$ est une relation d'équivalence, $\sigma'$ n'est pas en relation avec $\tau'$ et $\mathrm{Card}(\sigma' H \cap G\tau') = 0$. Supposons donc que $\mathrm{Card}(\sigma H \cap G\tau) \neq 0$, c'est-à-dire que $\tau \mathcal{R} \sigma$. Comme $\sigma' \in G\sigma H$, la classe à gauche $\sigma' H$ appartient à la $G$-orbite $\mathcal{O}$. Supposons que $\sigma H = \{u_1, \ldots, u_r\}$ et que $\sigma H \cap G\tau = \{u_1, \ldots, u_c\}$. Comme $\sigma' H \in \mathcal{O}$, nous avons $\sigma' H = \{gu_1, \ldots, gu_r\}$ où $g \in G$. Nous avons nécessairement $gu_1, \ldots, gu_c \in \sigma' H \cap G\tau$. Si, pour $s \in [\![1, r]\!]$, nous avons $gu_s \in \sigma' H \cap G\tau$ alors $h_s \in G\tau$ et alors $s \in [\![1, c]\!]$. Donc $c = \mathrm{Card}(\sigma' H \cap G\tau)$ et, comme il s'agit d'une relation d'équivalence, le résultat énoncé est vrai. □

*Notations* 6.5. Nous posons $c_\sigma = \mathrm{Card}(\sigma H \cap G\tau)$ pour tout $\tau \in (G\sigma H)$.

Le résultat suivant est illustré lors de l'exemple étudié au Paragraphe 7. Il donne, en particulier, une façon de pré-calculer les degrés des facteurs de la résolvante $R(\Theta, I)$.

THÉORÈME 6.6. *Nous avons*

$$\mathrm{Card}(G) = c_\sigma \, \mathrm{Card}(\mathcal{O});$$

*ce qui se traduit par*

$$\mathrm{Card}(G) = c_\sigma \, deg(h).$$

*Démonstration.* D'après le Lemme 6.3, nous avons

$$\sum_{i=1}^{d} (\sigma_i H \cap G\tau) = G\tau.$$

Comme cette union est disjointe, puisque les $\sigma_i H$ le sont deux-à-deux, nous avons

$$\sum_{i=1}^{d} \mathrm{Card}(\sigma_i H \cap G\tau) = \mathrm{Card}(G\tau) = \mathrm{Card}(G).$$

Pour finir, nous appliquons le Lemme 6.4 pour obtenir $d.\,\mathrm{Card}(\sigma H \cap G\tau) = \mathrm{Card}(G)$. □

THÉORÈME 6.7. *Supposons que la résolvante $R(\Theta, I)$ n'ait que des racines simples. Le nombre $m$ de facteurs $k$-irréductibles de la résolvante $R(\Theta, I)$ est le nombre de classes doubles distinctes $(G\sigma H)$ auxquelles appartiennent les permutations $\tau_1, \ldots, \tau_s$ telles que*

$$L = \mathrm{Inj}(I, \mathfrak{M}) = G\tau_1 + \cdots + G\tau_s.$$

*En particulier, $m \leq s$.*

*Démonstration.* Supposons $\theta^\sigma$ soit une racine de $R(\Theta, I)$. Alors le polynôme $h$ est un facteur simple de $R(\Theta, I)$ car $R(\Theta, I)$ n'a pas de racine multiple. Comme $h$ est sans racine multiple, ses racines $\theta^{\sigma_1}, \ldots, \theta^{\sigma_d}$ sont les éléments distincts de l'ensemble $\{\,(\theta^\sigma)^\tau \mid \tau \in G\}$. Par la théorie de Galois classique, le polynôme $h$ est donc $k$-irréductible; c'est le polynôme minimal de $\theta^\sigma$ sur $k$. D'après la Remarque 6.1, la classe double $(G\sigma H)$ est associée au facteur $h$. Donc, chaque facteur irréductible (simple) de la résolvante $R(\Theta, I)$ est associée à une et une unique classe double. Le Lemme 6.3 permet de conclure. □

*Remarque* 6.8. Nous retrouvons le résultat classique qui assure que si la résolvante possède un facteur simple $h = x - \theta^\sigma$ ($\sigma \in S_n$ étant forcément inconnu), alors $G \subset \sigma H \sigma^{-1}$. En effet, si c'est le cas alors $(G\sigma H) = \{\sigma H\}$. Dans la pratique, nous considérons $\underline{\alpha}$ tel que $h = x - \theta$ (i.e., $\sigma = \mathrm{id}$).

## 7. UN EXEMPLE D'APPLICATION

Nous considérons le polynôme $f = x^8 + x^4 + 2$ calculé par Mattman, McKay et Smith de groupe de Galois $8T_{26}$. En utilisant les résultats de [11], nous calculons des générateurs de l'idéal de Galois pur

$$I_M = \mathfrak{J} + \langle x_1x_2x_3x_4 + x_5x_6x_7x_8 - 1\rangle$$

de groupe de décomposition $M$, le sous-groupe de $S_8$ d'ordre 1152 et engendré par les permutations

$$a = (5,6), \quad b = (1,2), \quad c = (7,8), \quad d = (3,4),$$
$$e = (1,5)(2,6)(3,7)(4,8) \quad \text{et} \quad f = (2,3).$$

Pour calculer un ensemble triangulaire engendrant l'idéal $I_M$, nous utilisons l'implantation de P. Aubry en `AXIOM` pour décomposer un idéal en ensembles triangulaires (voir [2] et [3]). Nous obtenons trois ensembles triangulaires

engendrant respectivement trois idéaux de Galois $J_1, J_2$ et $J_3$ tels que

$$I_M = J_1 \cap J_2 \cap J_3.$$

En particulier, nous avons

$$J_1 = \langle x_1^8 + x_1^4 + 2,\ x_2 + x_1,\ x_3^2 + x_1^2,\ x_4 + x_3,\ x_5^4 + x_1^4 + 1, x_6^3 + x_6^2 x_5 + x_5^3,$$
$$x_7^2 + x_7 x_6 + x_7 x_5 + x_6^2 + x_6 x_5 + x_5^2,\ x_8 + x_7 + x_6 + x_5\rangle.$$

Pour chaque idéal $J_1, J_2$ et $J_3$, le produit de ses degrés initiaux est 384 (= 1152/3).

Soit $\mathfrak{M}$ un idéal maximal contenant $J_1$. Posons $L = \mathrm{Inj}(J_1, \mathfrak{M})$ et $L' = \mathrm{Inj}(J_2, \mathfrak{M}) \cup \mathrm{Inj}(J_3, \mathfrak{M}) = \mathrm{Inj}(J_1 \cap J_2, \mathfrak{M})$. Considérons le sous-groupe $H$ de $M$ d'ordre 128 et engendré par les permutations

$$bd, ac, cd, e, g = (1,3,2,4) \quad \text{et} \quad h = (5,7,6,8)$$

et le sous-groupe $G$ d'indice 2 dans $H$ et engendré par les permutations $bd, ac, e, g, h$ et $cd$.

*Remarque* 7.1. Les groupes $M$, $H$ et $G$ sont respectivement des conjugués des groupes $8T_{47}, 8T_{35}$ et $8T_{26}$.

Comme $G$ et $H$ sont deux sous-groupes d'indices respectifs 18 et 9 dans $M$, il existe des permutations $\tau_1 = \mathrm{id}, \ldots, \tau_{18}$, $\sigma_1 = \mathrm{id}, \ldots, \sigma_9$ de $M$ telles que nous ayons les deux unions disjointes

$$M = G\tau_1 + \cdots + G\tau_{18} = \sigma_1 H + \cdots + \sigma_9 H.$$

En numérotant correctement les permutations $\tau_j$, nous avons (voir Proposition 2.2)

$$L = G\tau_1 + \cdots + G\tau_6 \quad \text{et} \quad L' = G\tau_7 + \cdots + G\tau_{18}.$$

Le groupe $H$ est le stabilisateur dans $M$ du polynôme $\Theta = x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8$. Avec l'algorithme décrit dans [4], nous obtenons

$$M(\Theta, J_1) = x(x^4 - 4x^2 + 32)$$

et

$$M(\Theta, J_2) = M(\Theta, J_3) = (x^4 - 4x^2 + 32)(x^4 - 8x^2 - 112)$$

où $M(\Theta, I)$ est la forme sans facteur carré de la résolvante $R(\Theta, I)$ (i.e., le polynôme minimal de l'endomorphisme de multiplication par $\Theta$ dans $\mathbb{Q}[x_1, \ldots, x_n]/I$). La résolvante $R(\Theta, I_M)$ est de degré $e = 9$, l'indice de $H$ dans $M$, (voir (3.1)) et les polynômes $M(\Theta, J_1)$ et $M(\Theta, J_2)$ en sont des facteurs. Donc

$$R(\Theta, I_M) = x(x^4 - 4x^2 + 32)(x^4 - 8x^2 - 112).$$

La présence du facteur linéaire simple $x$ implique que le groupe de décomposition de $\mathfrak{M}$ (i.e., le groupe de Galois de $\underline{\alpha}$) est un sous-groupe de $H$ (voir Remarque 6.8).

Comme chaque résolvante $R(\Theta, J_i)$, $i \in \{1,2,3\}$, est aussi un facteur de $R(\Theta, M)$, nous avons $R(\Theta, J_i) = M(\Theta, J_i)$.

Ordonnons les permutations $\sigma_i$ pour que les facteurs de la résolvante $R_{\Theta, I_M}$ vérifient

$$h_1 = x = x - \theta^{\sigma_1}, \quad h_2 = x^4 - 4x^2 + 32 = \prod_{i=2}^{5}(x - \theta^{\sigma_i})$$

et

$$h_3 = x^4 - 8x^2 - 112 = \prod_{i=6}^{9}(x - \theta^{\sigma_i}).$$

Avec le Théorème 6.7, nous savons que

– $\tau_1, \ldots, \tau_6$ appartiennent aux deux classes doubles distinctes $(H\sigma_1 H)$ et $(H\sigma_2 H)$;

– $\tau_7, \ldots, \tau_{18}$ appartiennent aux deux classes doubles distinctes $(H\sigma_2 H)$ et $(H\sigma_6 H)$.

Le Théorème 6.6 explique de quelle manière les facteurs de la résolvante $R(\Theta, I_M)$ apparaissent dans les trois autres résolvantes $R(\Theta, J_i)$. Nous allons étudier le lien qui existe entre les trois résolvantes $R(\Theta, J_l)$ $(l \in \{1,2,3\})$ et les intersections $\sigma_i H \cap G\tau_j$ $(i \in [\![1,9]\!]$ et $j \in [\![1,18]\!])$.

Regardons d'abord la $G$-orbite de $\sigma_1 H$ (réduite à $\sigma_1 H$ puisque $G \subset H$) à laquelle le polynôme $h_1 = x$ est associé. Comme $\tau_1 = \sigma_1 = \mathrm{id}$, il vient $\tau_1 \in G\sigma_1 H$ et, d'après le Lemme 6.3, il s'en déduit $G\tau_1 = \sigma_1 H \cap G\tau_1$ (i.e. $G \subset H$). Nous avons

$$c_{\sigma_1} = \mathrm{Card}(\sigma_1 H \cap G\tau_1) = \mathrm{Card}(G) = 64.$$

Comme le polynôme $x$ n'est facteur que de la résolvante $R(\Theta, J_1)$, les 64 autres permutations de $\sigma_1 H$ appartiennent aussi à $L$. Choisissons la permutation $\tau_2$ de $L$ telle que $\sigma_1 H \cap G\tau_2 \neq \emptyset$. D'après le Lemme 6.4, il vient $c_{\sigma_1} = \mathrm{Card}(\sigma_1 H \cap G\,\tau_2)$. Nous avons $G\tau_2 = \sigma_1 H \cap G\tau_2$ (i.e. $G\tau_2 \subset H$). D'où $\tau_1, \tau_2 \in (G\sigma_1 H)$ et

$$H = (\sigma_1 H \cap G\,\tau_1) + (\sigma_1 H \cap G\,\tau_2) = G + G\tau_2.$$

Intéressons-nous maintenant à la $G$-orbite $\{\sigma_2 H, \ldots, \sigma_5 H\}$ à laquelle est associé le facteur $h_2$ commun aux trois résolvantes $R(\Theta, J_l)$, $l \in \{1,2,3\}$. Cette $G$-orbite est de cardinal $d = 4$. Pour $i \in \{2,3,4,5\}$ et $j \in \{3,4,5,6\}$, nous avons nécessairement $\tau_3, \ldots, \tau_6 \in (G\sigma_2 H)$ et $\sigma_i H \cap G\tau_j \neq \emptyset$ avec $c_{\sigma_2} = \mathrm{Card}(\sigma_i H \cap G\tau_j) = \mathrm{Card}(G)/d = 16$. Nous avons $4.c_{\sigma_2} = 64$ et $\mathrm{Card}(\sigma_2 H) = 2.64$. Il y a donc 64 permutations de $\sigma_2 H$ appartenant à $L$ (en fait à $G\tau_3 + G\tau_4 + G\tau_5 + G\tau_6$). Les 64 autres permutations de $\sigma_2 H$ appartiennent donc à $L'$. D'après les Lemmes 6.3 et 6.4, en numérotant correctement les $\tau_j$, nous

savons que les 4 classes à droites $G\tau_j$, $j \in \{7,8,9,10\}$, appartenant à $L'$ vérifient $\tau_j \in (G\sigma_2 H)$ et, pour $i \in \{2,3,4,5\}$, nous avons les trois égalités

$$G\tau_j = \sum_{i=2}^{5} \sigma_i H \cap G\tau_j, \quad c_{\sigma_2} = \mathrm{Card}(\sigma_i H \cap G\tau_j), \quad \sigma_i H = \sum_{j=3}^{10} (\sigma_i H \cap G\tau_j).$$

Le dernier facteur $h_3$ est associé à la $G$-orbite $\{\sigma_6 H, \ldots, \sigma_9 H\}$ de cardinal 4. Le polynôme $h_3$ est uniquement un facteur des résolvantes $R(\Theta, J_2)$ et $R(\Theta, J_3)$. Les 8 classes à droite $G\tau_{11}, \ldots, G\tau_{18}$ vérifient donc, pour $i \in \{6,7,8,9\}$ et $j \in [\![11,18]\!]$, les trois égalités

$$G\tau_j = \sum_{i=6}^{9} \sigma_i H \cap G\tau_j, \quad c_{\sigma_6} = \mathrm{Card}(\sigma_i H \cap G\tau_j) = 16, \quad \sigma_i H = \sum_{j=11}^{18} (\sigma_i H \cap G\tau_j).$$

Pour terminer, le groupe $H$ contient le groupe de Galois de $\underline{\alpha}$ tel que $\mathfrak{M}$ soit l'idéal des $\underline{\alpha}$-relations. Donc l'idéal de Galois $I_H$ défini par $H$ et $\mathfrak{M}$ est pur. Avec la permutation $e$ du groupe $H$, nous trouvons la relation $e.(x_1 + x_2) = x_5 + x_6$ qui appartient donc à $I_H$. L'idéal $J$ engendré par l'ensemble triangulaire (les 7-ième et 8-ième relations de $J_1$ ont été réduites avec $x_6 + x_5$):

$$T_H = \{x_1^8 + x_1^4 + 2,\ x_2 + x_1,\ x_3^2 + x_1^2,\ x_4 + x_3,\ x_5^4 + x_1^4 + 1,\ x_6 + x_5,\ x_7^2 + x_5^2,\ x_8 + x_7\}$$

est formé de relations de $J_1$ et de $I_H$. Il est donc inclus dans $I_H$. Le produit des degrés initiaux de $J$ étant 128, le cardinal de $H$, cet idéal s'identifie donc à $I_H$ (voir le Théorème 2.1). Nous retrouvons donc l'idéal pur attendu par le Théorème 5.3. Nous n'avons pas eu à vérifier que $L$ s'exprime sous la forme $L = HE$, avec $E$ un groupe; le calcul nous a donné directement de résultat voulu.

Pour calculer l'idéal maximal $\mathfrak{M}$, il existe plusieurs stratégies qui peuvent se combiner entre-elles:

(1) factoriser les relations restantes dans des sous-corps de $k(\alpha_1, \ldots, \alpha_8)$ déterminés par les générateurs de $I_H$ (voir [1]); on pourra s'aider des listes pré-calculées des degrés initiaux des idéaux de Galois attendus (voir [4]);
(2) utiliser l'algorithme `GaloisIdéal` de [11] qui est basé sur le calcul de résolvantes;
(3) si le groupe de Galois est déterminé comme étant $8T_{26}$, nous savons que nous cherchons à calculer une relation de la forme $x_7 + g(x_1, x_3, x_5)$ (voir [4]) où $\deg_{x_1}(g) < 8$, $\deg_{x_3}(g) < 2$ et $\deg_{x_5}(g) < 4$; ce calcul peut alors se réaliser en $p$-adique avec des coefficients inconnus que l'on cherche à déterminer (voir [13]).

En utilisant l'algorithme `GaloisIdéal` nous trouvons l'idéal des $\underline{\alpha}$-relations $\mathfrak{M}$ engendré par l'ensemble triangulaire

$$T_H \cup \{2x_7 + x_5x_3x_1^7 + x_5x_3x_1^3\} \backslash \{x_7^2 + x_5^2\}$$

de groupe de décomposition $G$, le groupe de Galois de $\underline{\alpha}$.

## 8. CONCLUSION

Nous avons exhibé des propriétés algébriques des racines des polynômes d'une variable en exploitant des propriétés des groupes finis. Comme souvent, l'étude sur les groupes s'est révélée bien plus simple que celle qu'on devrait mener directement sur les polynômes.

Avec l'application traitée au Paragraphe 7, les résultats de cet article apparaissent comme utiles au calcul de corps de décomposition et à l'étude des résolvantes.

**Remerciements.** Je remercie Antonio Machi de l'Université de Rome I, La Sapienza, pour m'avoir orientée vers l'utilisation des classes doubles dans l'étude des résolvantes.

REFERENCES

[1] H. Anai, M. Noro and K. Yokoyama, *Computation of the splitting fields and the Galois groups of polynomials.* In: *Algorithms in Algebraic Geometry and Applications* (*Santander*, 1994), pp. 29–50. Progress in Mathematics **143**. Birkhäuser, Basel, 1996.

[2] P. Aubry, *Ensembles triangulaires de polynômes et résolution de systèmes algébriques.* Ph.D. Thesis, Université Paris 6, 1999.

[3] P. Aubry and M. Moreno Mazat, *Triangular sets for solving polynomial systems: a comparative implantation of four methods*, J. Symbolic Comput. **28** (1999), 125–154.

[4] P. Aubry and A. Valibouze, *Using Galois ideals for computing relative resolvents.* J. Symbolic Comput. **30** (2000), *6*, 635–651.

[5] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system,* I. *The user language.* J. Symbolic Comput. **24** (1997), *3-4*, 235–265.

[6] A. Cauchy, *Usage des fonctions interpolaires dans la détermination des fonctions symétriques des racines d'une équation algébrique donnée.* Oeuvres **5**:473 Extrait 108, 1840.

[7] J.L. Lagrange, *Réflexions sur la résolution algébrique des équations.* Prussian Academy, 1770.

[8] S. Orange, G. Renault et A. Valibouze, *Calcul efficace de corps de décomposition.* Research Report LIP6 2003.005. Laboratoire d'Informatique de Paris 6, 2003. `http://www.lip6.fr/reports/lip6.2003.004.html`.

[9] N. Rennert et A. Valibouze, *Calcul de résolvantes avec les modules de Cauchy.* Experiment. Math. **8** (1999), *4*, 351–366.

[10] N. Tchebotarev, *Gründzüge des Galois'shen Theorie.* P. Noordhoff, 1950.

[11] A. Valibouze, *Étude des relations algébriques entre les racines d'un polynôme d'une variable.* Simon Stevin **6** (1999), *4*, 507–535.

[12] K. Yokoyama, *A modular method for computing the Galois groups of polynomials.* J. Pure Appl. Algebra **117/118** (1997), 617–636.
[13] K. Yokoyama, *A modular method to compute the splitting field of a polynomial.* Communication privée, 1999.

*Reçu le 15 février 2005*
*Révisé le 6 juin 2005*

*L.I.P.6 Université Paris VI*
*4, place Jussieu*
*75252 Paris Cedex 05, France*
*annick.valibouze@upmc.fr*