SCIENCES SORBONNE UNIVERSITÉ
FACULTÉ DES SCIENCES

ANNÉE 2017-2018

MASTER DE SCIENCES ET TECHNOLOGIES
MENTION MATHÉMATIQUES ET APPLICATIONS

CALCULS ALGÉBRIQUES - UE 4M021

RESPONSABLE : PIERRE CHAROLLOIS

Professeure :
ANNICK VALIBOUZE

Cours 10 et 12

Table des matières

COURS 10

1. Introduction aux idéaux galoisiens et quelques notations

Jusqu'à la fin du cours, nous abordons la théorie de Galois dite "constructive". Nous considérerons des idéaux particuliers appelés "galoisiens ". Deux d'entre eux furent introduits en 1950 par N. Tcheboratrev dans son livre "Gründzüge des Galois'shen Theorie" (Ed. P. Noordhoff) : l'"idéal des relations symétriques" engendré par les "modules de Cauchy" et l'"idéal des $\boldsymbol{\alpha}$*-relations" engendré par les "modules fondamentaux". Nous devons ces dénominations à N. Tchebotarev. Lorsque que le polynôme d'une variable de départ est sans racine multiple, les modules de Cauchy et fondamentaux sont chacun, par construction, des ensembles triangulaires séparables. La forme générale d'un idéal galoisien fut introduite bien plus tard en 1995 (voir "Theory of Equations, Lagrange and Galois Theory", AV, https ://cel.archives-ouvertes.fr/cel-00403452v1). Ce sont tous les idéaux radicaux entre l'idéal des relations symétriques et les idéaux de relations qui sont maximaux. Un autre outil fondamental de la théorie de Galois "constructive" est la résolvante introduite par J.L. Lagrange dans le cas particulier de celle dite "absolue". Nous allons étudier comment les idéaux galoisiens et les résolvantes offrent un moyen à la fois simple et calculatoire d'aborder la théorie de Galois.*

Données

Nous fixons le corps $k := \mathbb{Q}$ (ou tout corps parfait) et un polynôme f (unitaire) d'une variable x :

$$f(x) := (x-\alpha_1)\cdots(x-\alpha_n) \in k[x]$$

à coefficients dans k.Les racines $\alpha_1,\ldots,\alpha_n$ de f sont supposées deux-à-deux distinctes. Le polynôme f est alors dit *séparable* ou sans facteur carré ou encore sans facteur multiple. Fixons un n-uplet $\boldsymbol{\alpha} := (\alpha_1,\ldots,\alpha_n)$ de ses racines.

Nous considérerons l'*idéal des* $\boldsymbol{\alpha}$*-relations*

$$\mathfrak{M}_{\boldsymbol{\alpha}} := \{r \in k[\boldsymbol{x}] \mid r(\boldsymbol{\alpha}) = 0\} = \mathrm{Id}_k(\boldsymbol{\alpha}) \quad . \tag{1}$$

Notre objectif est de réaliser des calculs algébriques avec les racines de f. Nous verrons que pour y parvenir, il nous faudra trouver des générateurs de $\mathfrak{M}_{\boldsymbol{\alpha}}$, appelés "modules fondamentaux" et formant un ensemble triangulaire séparable.

L'anneau $k[\boldsymbol{\alpha}]$ est identique à son corps des fractions $k(\boldsymbol{\alpha})$, le corps des racines du polynôme f appelé aussi son *corps de décomposition*. L'identité $k[\boldsymbol{\alpha}] = k(\boldsymbol{\alpha})$ se montre par récurrence, en débutant par l'identité $k[\alpha_1] = k(\alpha_1)$. Cette identité se montre classiquement à partir du polynôme minimal h de α_1 sur k (polynôme unitaire irréductible sur k tel que $h(\alpha_1) = 0$) : soit $0 \neq v \in k(\alpha_1)$; il existe $p \in k[x]$ avec $\deg(p) < \deg(h)$ tel que $v = p(\alpha_1)$; en évaluant en α_1 l'identité de Bézout : $q(x)p(x) + g(x)h(x) = \mathrm{pgcd}(p,h) = 1$, nous trouvons $w = q(\alpha_1)$, l'inverse de v.

Groupes et actions de groupes - Rappels

Nous notons S_n le groupe symétrique de degré n.

Pour $\sigma, \tau \in S_n$, et $p \in k[\boldsymbol{x}]$, posons $\sigma \cdot p := p(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ et $\boldsymbol{\alpha}^\sigma := (\alpha_{\sigma(1)}, \ldots \alpha_{\sigma(n)})$.

Soit $L \subset S_n$. Pour P un ensemble de polynômes de $k[\boldsymbol{x}]$ et $p \in P$, nous posons : $\sigma \cdot P := \{\sigma \cdots p \mid p \in P\}$, $L \cdot p := \{\sigma \cdot p \mid \sigma \in L\}$ et

$$L \cdot P := \bigcup_{\sigma \in L} \sigma \cdot P = \bigcup_{p \in P} L \cdot p \qquad .$$

L'ensemble $L \cdot p$ de polynômes de $k[\boldsymbol{x}]$ est appelé la L-*orbite* de p sous l'action de L.

De même, pour E un ensemble de n-uplets et $e \in E$, nous posons : $E^\sigma := \{e^\sigma \mid e \in E\}$, $e^L := \{e^\sigma \mid \sigma \in L\}$, la L-*orbite* de e sous l'action de L, et

$$E^L := \bigcup_{\sigma \in L} E^\sigma = \bigcup_{e \in E} e^L \qquad .$$

Afin d'alléger la présentation, nous userons de cette notation : $L \star e := e^L$ pour désigner l'orbite du n-uplet e sous l'action de L. Nous avons :

$$(\boldsymbol{\alpha}^\tau)^\sigma \quad = \quad \boldsymbol{\alpha}^{\tau\sigma} \tag{2}$$

En effet, fixons $i \in [\![1, n]\!]$ et posons $\boldsymbol{\beta} := \boldsymbol{\alpha}^\tau$, i.e. $\beta_j := \alpha_{\tau(j)}$ pour $j \in [\![1, n]\!]$. Pour j tel que $j = \sigma(i)$, il vient : $\beta_{\sigma(i)} = \beta_j = \alpha_{\tau(j)} = \alpha_{\tau(\sigma(i))}$; soit $(\boldsymbol{\alpha}^\tau)^\sigma = \boldsymbol{\beta}^\sigma = \boldsymbol{\alpha}^{\tau\sigma}$.

Afin d'alléger la présentation, nous userons de cette notation : $\sigma \cdot p(\boldsymbol{\alpha}) := (\sigma \cdot p)(\boldsymbol{\alpha})$ où $(\sigma \cdot p)(\boldsymbol{\alpha}) = p(\boldsymbol{\alpha}^\sigma) = p(\alpha_{\sigma(1)}, \ldots \alpha_{\sigma(n)})$. Pour éviter les confusions, vérifions que :

$$\sigma \cdot p(\boldsymbol{\alpha}^\tau) \quad = \quad p(\boldsymbol{\alpha}^{\tau\sigma}) = \tau\sigma \cdot p(\boldsymbol{\alpha}) \qquad . \tag{3}$$

En effet, $(\sigma \cdot p)(\boldsymbol{\alpha}^\tau) = p((\boldsymbol{\alpha}^\tau)^\sigma) = p(\boldsymbol{\alpha}^{\tau\sigma})$, d'après (2).

2. Idéal des relations symétriques

Considérons l'ensemble $\mathfrak{S}$ des polynômes de $k[\boldsymbol{x}]$ qui s'annulent sur l'orbite de $\boldsymbol{\alpha}$ sous l'action du groupe symétrique S_n :

$$\mathfrak{S} = \{r \in k[\boldsymbol{x}] \mid \forall \sigma \in \mathrm{S}_n \quad \sigma \cdot r(\boldsymbol{\alpha}) = 0\} \quad .$$

Cet ensemble est clairement un idéal radical qui se définit aussi comme celui de l'orbite $\mathrm{S}_n \star \boldsymbol{\alpha}$ de $\boldsymbol{\alpha}$ sous l'action de S_n :

$$\mathfrak{S} := \mathrm{Id}_k(\mathrm{S}_n \star \boldsymbol{\alpha}) \quad . \tag{4}$$

Cet idéal $\mathfrak{S}$ est appelé l'*idéal des relations symétriques* entre les racines du polynôme univarié f. Il ne dépend clairement pas de l'ordre des racines choisi pour le n-uplet $\boldsymbol{\alpha}$ des racines de f.

EXEMPLE 2.1. Soit $s \in k[\boldsymbol{x}]$, un polynôme symétrique en $x_1, \ldots, x_n$. Nous avons $s(\boldsymbol{\alpha}) \in k$ par le théorème fondamental des fonctions symétriques. Ainsi $s(\boldsymbol{x}) - s(\boldsymbol{\alpha}) \in \mathfrak{S}$. Le polynôme $f(x_1) - f(\alpha_1)$ est également une relation symétrique ; i.e. appartient à $\mathfrak{S}$. Pourtant il n'est pas symétrique en $x_1, \ldots, x_n$.

L'exemple précédent nous enseigne qu'il ne faut donc pas confondre les relations symétriques et les polynômes symétriques. Néanmoins, nous verrons que certaines relations symétriques offrent une version effective du théorème fondamental des fonctions symétriques ; c'est-à-dire qu'elles permettent d'obtenir la valeur dans k du polynôme symétrique s évalué en les n racines de f.

La variété $\mathrm{V}(\mathfrak{S})$ de l'idéal des relations symétriques est donnée par :

$$\mathrm{V}(\mathfrak{S}) = \mathrm{S}_n \star \boldsymbol{\alpha} = \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \mid \sigma \in \mathrm{S}_n\} \quad . \tag{5}$$

DÉMONSTRATION. En effet, l'ensemble $\mathscr{J}_f := \{s_1(\boldsymbol{x}) - s_1(\boldsymbol{\alpha}), \ldots, s_n(\boldsymbol{x}) - s_n(\boldsymbol{\alpha})\}$ de polynômes de $k[\boldsymbol{x}]$ où s_i est la i-ième fonction symétrique élémentaire, est inclus dans l'idéal $\mathfrak{S}$ (voir Exemple 2.1). Or l'ensemble des zéros $\boldsymbol{\beta}$ de $\mathscr{J}_f$ est $\mathrm{S}_n \star \boldsymbol{\alpha}$; en effet, $s_i(\boldsymbol{\beta}) = s_i(\boldsymbol{\alpha})$ si et seulement si $\prod_{i=1}^n (x - \beta_i) = \prod_{i=1}^n (x - \alpha_i)$ qui est équivalent à ce que $\boldsymbol{\beta}$ soit une permutation de $\boldsymbol{\alpha}$. Donc $\mathrm{V}(\mathfrak{S}) \subset \mathrm{S}_n \star \boldsymbol{\alpha}$. On en déduit l'égalité puisque $\mathrm{S}_n \star \boldsymbol{\alpha} \subset \mathrm{V}(\mathrm{Id}_k(\mathrm{S}_n \star \boldsymbol{\alpha})) = \mathrm{V}(\mathfrak{S})$, par définition de l'idéal $\mathfrak{S}$. □

Définissons l'ensemble $\mathbf{C} = \{\mathrm{C}_{1,\boldsymbol{\alpha}}, \ldots, \mathrm{C}_{n,\boldsymbol{\alpha}}\}$, formé des *n modules de Cauchy de f* dans $k[\boldsymbol{x}]$. Pour simplifier, nous posons $\mathrm{C}_i := \mathrm{C}_{i,\boldsymbol{\alpha}}$ et ci-dessous nous définissons inductivement les modules de Cauchy :

$$\begin{aligned}
\mathrm{C}_n(x_n) &:= f(x_n)\\
\mathrm{C}_{n-1}(x_{n-1},x_n) &:= \frac{\mathrm{C}_n(x_{n-1})-\mathrm{C}_n(x_n)}{x_{n-1}-x_n}\\
&\vdots\\
\mathrm{C}_r(x_r,\ldots,x_n) &:= \frac{\mathrm{C}_{r+1}(x_r,x_{r+2},\ldots,,x_n)-\mathrm{C}_{r+1}(x_{r+1},x_{r+2},\ldots,,x_n)}{x_r-x_{r+1}} \quad 1\le r<n
\end{aligned}$$

Par substitutions, nous avons, pour tout $\boldsymbol{\beta}\in \mathrm{V}(\mathfrak{S})$:

$$\begin{aligned}
\mathrm{C}_n(x_n)=f(x_n) &= (x_n-\beta_1)(x_n-\beta_2)\cdots(x_n-\beta_{n-1})(x_n-\beta_n)\\
\mathrm{C}_{n-1}(x_{n-1},\beta_n) &= (x_{n-1}-\beta_1)(x_{n-1}-\beta_2)\cdots(x_{n-1}-\beta_{n-1})\\
&\vdots\\
\mathrm{C}_r(x_r,\beta_{r+1},\ldots,\beta_{n-1},\beta_n) &= (x_r-\beta_1)\cdots(x_r-\beta_r) \qquad (6)\\
&\vdots\\
\mathrm{C}_1(x_1,\beta_2,\ldots,\beta_n) &= x_1-\beta_1 \quad .
\end{aligned}$$

D'où

$$\mathrm{V}(\mathbf{C})=\mathrm{S}_n\star\boldsymbol{\beta}=\mathrm{V}(\mathfrak{S}) \quad .$$

Puisque $\mathrm{C}_r=x_r^r+g_r(x_r,\ldots,x_n)$ avec $\deg_{x_r}(g_r)<r$, l'ensemble $\mathbf{C}$ formé des modules de Cauchy est un *ensemble triangulaire* et réduit, par construction. Il est *séparable* puisque les racines de f sont deux-à-deux disjointes (cela se voit sur (6)). Puisqu'il est triangulaire séparable, il est radical (voir cours suivant). Puisque les idéaux $\mathfrak{S}$ et $<\mathrm{C}_1,\ldots,\mathrm{C}_n>$ sont tous deux radicaux (avec $\mathrm{V}(\{\mathrm{C}_1,\ldots,\mathrm{C}_n\})=\mathrm{V}(\mathfrak{S})$, il vient :

THÉORÈME 1. *Soit f un polynôme séparable. Alors l'idéal $\mathfrak{S}$ de ses relations symétriques est triangulaire et engendré par les modules de Cauchy :*

$$\mathfrak{S}=<\mathrm{C}_1,\ldots,\mathrm{C}_n> . \qquad (7)$$

Les n polynômes $\mathcal{V}_r:=\sum_{i=0}^{r}a_i h_{r-i}(x_r,\ldots,x_n)$, $r\in[\![1,n]\!]$, satisfont ces n identités :

$$\mathrm{C}_r=\mathcal{V}_r \quad r=1,\ldots,n \qquad (8)$$

où $h_i(\boldsymbol{y})$ est la somme des monômes de poids i en les variables de $\boldsymbol{y}$ et $a_i:=(-1)^i s_i(\boldsymbol{\alpha})$, s_i étant la i-ième fonction symétrique élémentaire en $x_1,\ldots,x_n$.

REMARQUE 2. On voit sur les polynômes $\mathcal{V}_1,\ldots,\mathcal{V}_n$ qu'ils sont "réduits" puisque de la forme : $\mathcal{V}_r = x_r^r + \mathrm{G}_r(x_r,\ldots,x_n)$ avec $\deg_{x_j}(\mathrm{G}_r) < j = \deg_{x_j}(\mathcal{V}_j)$ pour tout $j \in [\![1,n]\!]$.

EXEMPLE 2.2. Les modules de Cauchy du polynôme $f := x^4 - 2x^3 + 2x^2 + 2$ sont :

$$\begin{aligned}
\mathrm{C}_4(x_4) &= x_4^4 - 2x_4^3 + 2x_4^2 + 2 = f(x_4)\\
\mathrm{C}_3(x_3,x_4) &= x_3^3 + x_4x_3^2 + x_4^2x_3 + x_4^3 - 2(x_3^2 + x_4x_3 + x_4^2) + 2(x_3 + x_4)\\
\mathrm{C}_2(x_2,x_3,x_4) &= x_2^2 + x_2x_3 + x_3^2 + x_2x_4 + x_3x_4 + x_4^2 - 2(x_2 + x_3 + x_4) + 2\\
\mathrm{C}_1(x_1,x_2,x_3,x_4) &= x_1 + x_2 + x_3 + x_4 - 2 \quad .
\end{aligned}$$

Les modules de Cauchy ont été exprimés à l'aide des polynômes $\mathcal{V}_1,\ldots,\mathcal{V}_4$. Ces polynômes non symétriques appartiennent chacun à l'idéal des relations symétriques $\mathfrak{S}$. Par exemple, pour toute permutation σ, $\sigma\cdot\mathrm{C}_4(\boldsymbol{\alpha}) = f(\alpha_{\sigma(4)}) = 0$.

Remarque : Soit $\mathscr{J}_f := \{s_1(\boldsymbol{x}) - s_1(\boldsymbol{\alpha}),\ldots,s_n(\boldsymbol{x}) - s_n(\boldsymbol{\alpha})\}$. Puisque f est sans racine double, nous avons pu attester que $\mathfrak{S} =< \mathbf{C} >$; en fait, nous avons

$$\mathfrak{S} =< \mathscr{J}_f >=< \mathbf{C} > .$$

DÉMONSTRATION. Pour le démontrer, posons $\mathrm{I} =< \mathscr{J}_f >$ et partons de la preuve de $\mathrm{V}(\mathfrak{S}) = \mathrm{S}_n \star \boldsymbol{\alpha}$ qui montre aussi que $\mathrm{V}(\mathrm{I}) = \mathrm{V}(\mathfrak{S})$. Donc $\mathrm{I} \subset \sqrt{\mathrm{I}} = \mathfrak{S} =< \mathbf{C} >$. Soient $\mathrm{C}_r = \mathrm{C}_{r,\boldsymbol{\alpha}}$ le r-ième module de Cauchy de f et $\mathrm{C}_{r,\boldsymbol{x}}$ celui de $\prod_{i=1}^n (x - x_i)$. Puisque $\mathrm{C}_{r,\boldsymbol{x}}(x_r,\ldots,x_n) = 0$ (les modules de Cauchy s'annulent en les racines du polynôme qui les définit), en appliquant la formule (8) à $\mathrm{C}_{r,\boldsymbol{x}}$ et à $\mathrm{C}_{r,\alpha}$, nous obtenons

$$\mathrm{C}_{r,\alpha} = \mathrm{C}_{r,\alpha} - \mathrm{C}_{r,\boldsymbol{x}} = q_1(s_1(\boldsymbol{x}) - s_1(\boldsymbol{\alpha})) + \cdots + q_r(s_r(\boldsymbol{x}) - s_r(\boldsymbol{\alpha})) \in \mathrm{I} \tag{9}$$

où $q_i = (-1)^{i+1} h_{r-i}(x_r,\ldots,x_n)$ pour $i \in [\![1,r]\!]$. D'où $\mathbf{C} \subset \mathrm{I}$ et nous avons bien l'égalité $\mathfrak{S} =< \mathbf{C} >=< \mathscr{J}_f >$ lorsque f est sans racine multiple. □

En toute généralité, que f possède ou non une racine double, l'identité $< \mathbf{C} >=< \mathscr{J}_f >$ demeure satisfaite. Cette identité n'étant pas nécessaires au déroulé du cours, nous ne la démontrerons pas. De plus, si f possède au moins une racine double alors $< \mathbf{C} >=< \mathscr{J}_f > \subsetneq \mathfrak{S}$; en effet, si $\overline{f}$ est la forme sans facteur carré de f alors $\overline{f}(x_n)$ est une relation symétrique qui ne se réduit pas à zéro modulo $\mathbf{C}$ (car sa réduction est elle-même).

Le groupe symétrique S_n est le *stabilisateur* de l'idéal des relations symétriques :

$$\mathrm{S}_n = \mathrm{Stab}(\mathfrak{S}) = \{\sigma \in \mathrm{S}_n \mid \sigma\cdot\mathfrak{S} \subseteq \mathfrak{S}\} \tag{10}$$

(preuve évidente) et, par définition de $\mathfrak{S}$, nous avons également :

$$S_n = \{\sigma \in S_n \mid \sigma \cdot \mathfrak{S} \subseteq \mathfrak{M}_{\boldsymbol{\alpha}}\}$$

(i.e. S_n envoie $\mathfrak{S}$ dans $\mathfrak{M}_{\boldsymbol{\alpha}}$) où $\mathfrak{M}_{\boldsymbol{\alpha}}$ est l'idéal des α-relations :

$$\mathfrak{M}_{\boldsymbol{\alpha}} := \{r \in k[\boldsymbol{x}] \mid r(\boldsymbol{\alpha}) = 0\} = \mathrm{Id}_k(\boldsymbol{\alpha}) \quad . \tag{11}$$

Nous verrons en TD que la réduction d'un polynôme symétrique modulo les modules de Cauchy fournit une nouvelle méthode effective du théorème fondamental des fonctions symétriques.

3. Idéal des relations et corps des racines du polynôme f

L'idéal $\mathfrak{M}_{\boldsymbol{\alpha}}$ des $\boldsymbol{\alpha}$-relations est le noyau du morphisme d'algèbre surjectif d'évaluation suivant :

$$\begin{array}{rcl} \psi : k[\boldsymbol{x}] & \longrightarrow & k[\boldsymbol{\alpha}] = k(\boldsymbol{\alpha}) \\ p(\boldsymbol{x}) & \longmapsto & p(\boldsymbol{\alpha}) \quad . \end{array}$$

Ce morphisme induit donc un isomorphisme entre l'anneau quotient $A := k[\boldsymbol{x}]/\mathfrak{M}_{\boldsymbol{\alpha}}$ et le corps $k(\boldsymbol{\alpha})$:

$$k[\boldsymbol{x}]/\mathfrak{M}_{\boldsymbol{\alpha}} \simeq k(\boldsymbol{\alpha}) \quad .$$

REMARQUE 3. Le fait que l'idéal $\mathfrak{M}_{\boldsymbol{\alpha}}$ soit maximal est équivalent à ce que l'algèbre $k[\boldsymbol{x}]/\mathfrak{M}_{\boldsymbol{\alpha}}$ soit un corps ; i.e. que $k[\boldsymbol{\alpha}] = k(\boldsymbol{\alpha})$. Nous pouvons donc prouver des deux propriétés à partir de l'autre : à savoir $k[\boldsymbol{\alpha}] = k(\boldsymbol{\alpha})$ et $\mathfrak{M}_{\boldsymbol{\alpha}}$ est maximal.

L'idéal des $\boldsymbol{\alpha}$-relations $\mathfrak{M}_{\boldsymbol{\alpha}}$ est triangulaire : il est engendré par un ensemble triangulaire séparable réduit formé par les *modules fondamentaux*

$$\mathfrak{F}_1(x_1, \ldots x_n), \ldots, \mathfrak{F}_n(x_n) \quad \text{avec } \mathfrak{F}_i \in k[x_i, \ldots, x_n]$$

appelés ainsi par Tchebotarev qui les définit inductivement comme suit : posons $k_{n+1} := k$ et $k_i := k_{i+1}(\alpha_i) = k(\alpha_{i+1}, \ldots, \alpha_n)$. Pour tout $i \in [\![1, n]\!]$, $\mathfrak{F}_i(x_i, \alpha_{i+1}, \ldots, \alpha_n) = \min_{\alpha_i, k_{i+1}}(x_i)$. On a ainsi $k_i \simeq k[x_i, \ldots, x_n]/ < \mathfrak{F}_i, \ldots, \mathfrak{F}_n >$. Les modules fondamentaux se calculent naturellement par factorisations successives de f dans les extensions k_i. (voir aussi Cours 9)

L'ensemble de permutations :

$$\mathrm{G}_{\boldsymbol{\alpha}} := \mathrm{Stab}(\mathfrak{M}_{\boldsymbol{\alpha}}) = \{\sigma \in \mathrm{S}_n \mid \sigma \cdot \mathfrak{M}_{\boldsymbol{\alpha}} \subseteq \mathfrak{M}_{\boldsymbol{\alpha}}\} \tag{12}$$

qui envoie toute $\boldsymbol{\alpha}$-relation sur une $\boldsymbol{\alpha}$-relation est le *stabilisateur* de $\mathfrak{M}_{\boldsymbol{\alpha}}$.

Ce stabilisateur $\mathrm{G}_{\boldsymbol{\alpha}}$ est un sous-groupe de S_n car il est à la fois fini, non vide (il contient l'identité) et stable par composition interne comme nous le montrons maintenant. Soient $\tau, \sigma \in \mathrm{G}_{\boldsymbol{\alpha}}$ et $r \in \mathfrak{M}_{\boldsymbol{\alpha}}$. Alors $\sigma\tau \cdot \mathfrak{M}_{\boldsymbol{\alpha}} = \sigma \cdot (\tau \cdot \mathfrak{M}_{\boldsymbol{\alpha}}) \subseteq \sigma \cdot \mathfrak{M}_{\boldsymbol{\alpha}} \subseteq \mathfrak{M}_{\boldsymbol{\alpha}}$, par définition de $\mathrm{G}_{\boldsymbol{\alpha}}$. Ainsi $\sigma\tau \in \mathrm{G}_{\boldsymbol{\alpha}}$.

Le groupe $\mathrm{G}_{\boldsymbol{\alpha}}$ est appelé le *groupe de Galois* de $\boldsymbol{\alpha}$ sur k et sera parfois noté $\mathrm{Gal}_k(\boldsymbol{\alpha}) := \mathrm{G}_{\boldsymbol{\alpha}}$ (pour certaines identités fondamentales).

La variété algébrique $\mathrm{V}(\mathfrak{M}_{\boldsymbol{\alpha}})$ définie comme l'ensemble des zéros de l'idéal $\mathfrak{M}_{\boldsymbol{\alpha}}$ est l'orbite du n-uplets $\boldsymbol{\alpha}$ sous l'action de son groupe de Galois sur k :

$$\mathrm{V}(\mathfrak{M}_{\boldsymbol{\alpha}}) = \mathrm{Gal}_k(\boldsymbol{\alpha}) \star \boldsymbol{\alpha} \quad . \tag{13}$$

DÉMONSTRATION. En effet, $\mathfrak{S} \subset \mathfrak{M}_{\boldsymbol{\alpha}}$ puisque l'identité appartient à S_n ; nous avons donc $\mathrm{V}(\mathfrak{M}_{\boldsymbol{\alpha}}) \subset \mathrm{S}_n \star \boldsymbol{\alpha} = \mathrm{V}(\mathfrak{S})$. Soit $\boldsymbol{\alpha}^\sigma \in \mathrm{V}(\mathfrak{M}_{\boldsymbol{\alpha}})$, avec $\sigma \in \mathrm{S}_n$. Alors, par définition de l'ensemble des zéros d'un ensemble de polynômes, pour tout $r \in \mathfrak{M}_{\boldsymbol{\alpha}}$ nous avons $0 = r(\boldsymbol{\alpha}^\sigma) = \sigma \cdot r(\boldsymbol{\alpha})$. Donc $\sigma \in \mathrm{G}_{\boldsymbol{\alpha}}$, par définition de $\mathrm{G}_{\boldsymbol{\alpha}}$. □

En conséquence, d'après (13),

$$\mathfrak{M}_{\boldsymbol{\alpha}} = \mathrm{Id}_k(\boldsymbol{\alpha}) = \mathrm{Id}_k(\mathrm{H} \star \boldsymbol{\alpha}) = \mathrm{Id}_k(\mathrm{Gal}_k(\boldsymbol{\alpha}) \star \boldsymbol{\alpha}) \qquad \forall \mathrm{H} \subset \mathrm{Gal}_k(\boldsymbol{\alpha}) \tag{14}$$

et les racines de f étant deux-à-deux distinctes, le cardinal de la variété de l'idéal des $\boldsymbol{\alpha}$-relations s'identifie à l'ordre (i.e. le cardinal) du groupe de Galois de $\boldsymbol{\alpha}$ sur k :

$$\mathrm{Card}(\mathrm{V}(\mathfrak{M}_{\boldsymbol{\alpha}})) = \mathrm{Card}(\mathrm{Gal}_k(\boldsymbol{\alpha})) \quad . \tag{15}$$

L'anneau A est une algèbre car aussi un espace vectoriel sur k. Rappelons que les multiplicités des zéros d'un idéal radical sont toutes identiques à 1. L'idéal $\mathfrak{M}$ étant radical, nous avons $\dim_k \mathrm{A} = \mathrm{Card}(\mathrm{V}(\mathfrak{M}))$ qui conduit à cette égalité fondamentale de la théorie de Galois entre l'ordre du groupe de Galois sur k et la dimension de A en tant qu'espace-vectoriel sur k :

$$\dim_k k(\boldsymbol{\alpha}) = \mathrm{Card}(\mathrm{Gal}_k(\boldsymbol{\alpha})) \quad . \tag{16}$$

Action du groupe de Galois sur le corps $k(\boldsymbol{\alpha})$

Le groupe de Galois $\mathrm{G}_{\boldsymbol{\alpha}}$ est l'ensemble maximal de permutations permettant de définir une action sur $k[\boldsymbol{\alpha}] = k(\boldsymbol{\alpha})$.

Par exemple, si $\alpha_1 = 1$ est racine de $f = x^3 + 1$, nous montrons facilement que pour la relation $r := \alpha_2^3 - \alpha_1$ et $\tau = (1,3)$ alors il n'y a pas d'action fidèle sur $\beta = \alpha_2^3 = \alpha_1$ car $\tau \cdot r \neq 0$ (i.e. $\tau \notin \mathrm{Gal}_k(\boldsymbol{\alpha})$).

De manière générale, soient $\Theta, \Psi \in k[\boldsymbol{x}]$ tels que $\Theta(\boldsymbol{\alpha}) = \Psi(\boldsymbol{\alpha})$ alors $(\Theta - \Psi)(\boldsymbol{\alpha}) = 0$; i.e. $\Theta - \Psi \in \mathfrak{M}_{\boldsymbol{\alpha}}$ et on n'est assuré de $\sigma \cdot \Theta(\boldsymbol{\alpha}) = \sigma \cdot \Psi(\boldsymbol{\alpha})$ que pour $\sigma \in \mathrm{G}_{\boldsymbol{\alpha}}$, par définition de $\mathrm{G}_{\boldsymbol{\alpha}}$. Notons que lorsque les racines de f sont "algénriquement indépendantes", des "variables", le groupe de Galois est alors S_n et nous savons que si deux polynômes sont identiques : $\mathrm{P} = \mathrm{Q}$ alors $\sigma \cdot \mathrm{P} = \sigma \cdot \mathrm{Q}$ toute permutation $\sigma \in \mathrm{S}_n$.

Soit $\theta \in k(\boldsymbol{\alpha})$ et un polynôme $\Theta \in k[\boldsymbol{x}]$ tel que $\theta := \Theta(\boldsymbol{\alpha})$. Pour tout $\sigma \in \mathrm{G}_{\boldsymbol{\alpha}}$, nous pouvons adopter cette notation pour l'action de σ sur θ :

$$\theta^\sigma := \sigma \cdot \Theta(\boldsymbol{\alpha}) = \Theta(\boldsymbol{\alpha}^\sigma) \quad . \tag{17}$$

Le *groupe de Galois* G *de* f *sur* k, appelé aussi de $k(\boldsymbol{\alpha})$ sur k, est classiquement défini comme le groupe des k-automorphisme de $k(\boldsymbol{\alpha})$ dans $k(\boldsymbol{\alpha})$. Il y a un morphisme naturel entre le groupe de Galois $\mathrm{Gal}_k(\boldsymbol{\alpha})$ et G qui à $\sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})$ associe $\phi_\sigma \in \mathrm{G}$ défini par $\phi_\sigma(\theta) = \theta^\sigma$ pour tout $\sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})$.

4. Les théorèmes fondamentaux de Galois

Ayant déterminé la variété de $\mathfrak{M} := \mathfrak{M}_{\boldsymbol{\alpha}}$, pour tout polynôme $\Theta \in k[\boldsymbol{x}]$, nous pouvons exprimer le polynôme caractéristique $\chi_{\hat{\Theta},\mathfrak{M}}$ de $\hat{\Theta}$, l'endomorphisme multiplicatif de $k[\boldsymbol{x}]/\mathfrak{M}$ induit par Θ :

$$\chi_{\hat{\Theta},\mathfrak{M}}(x) = \prod_{\boldsymbol{\beta} \in \mathrm{V}(\mathfrak{M})} (x - \Theta(\boldsymbol{\beta})) = \prod_{\sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})} (x - \sigma \cdot \Theta(\boldsymbol{\alpha})) \tag{18}$$

et nous avons tout naturellement $\chi_{\hat{\Theta},\mathfrak{M}}(x) \in k[x]$ (puisque $\mathfrak{M}$ est radical, toutes les multiplicités des éléments de la variété sont identiques à 1). Le polynôme caractéristique

s'exprime aussi ainsi :

$$\chi_{\hat{\Theta},\mathfrak{M}}(x) = \prod_{\sigma\in \mathrm{Gal}_k(\boldsymbol{\alpha})} (x-\theta^\sigma) \quad .$$

THÉORÈME 4. *(Galois) Soit* $\gamma \in k(\boldsymbol{\alpha})$. *Pour que* $\gamma \in k$ *il faut et il suffit que que* $\gamma^\sigma = \gamma$ *pour tout* $\sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})$.

DÉMONSTRATION. Les outils que nous avons mis en place, nous offrent une preuve simple du théorème de Galois. Notons que l'action de permutations sur les éléments de $k(\boldsymbol{\alpha})$ est bien définie seulement pour les permutation du groupe de Galois. Soit $\Gamma \in k[\boldsymbol{x}]$ tel que $\gamma = \Gamma(\boldsymbol{\alpha})$. Si $\gamma \in k$ alors le polynôme $r := \Gamma(\boldsymbol{x}) - \gamma$ de $k[\boldsymbol{x}]$ est une $\boldsymbol{\alpha}$-relation. Donc, par définition du groupe de Galois, pour tout $\sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})$, $\sigma \cdot r(\boldsymbol{\alpha}) = 0$; ce qui signifie que $\gamma^\sigma = \gamma$. Inversement, supposons que $\gamma^\sigma = \gamma$ pour les d permutations de $\mathrm{Gal}_k(\boldsymbol{\alpha})$. Alors, $\chi_{\hat{\Gamma},\mathfrak{M}}(x) = (x-\gamma)^d \in k[x]$. Comme k est un corps parfait, nous avons bien $\gamma \in k$. □

REMARQUE 5. Rappelons, que le corps k étant parfait et l'idéal $\mathfrak{M}$ étant radical, le polynôme minimal $\mathrm{M}_{\hat{\Theta},\mathfrak{M}}$ de l'endomorphisme $\hat{\Theta}$ qui appartient à $k[x]$ s'identifie à la forme sans facteur carré du polynôme caractéristique (A faire en exercice). D'où :

$$\mathrm{M}_{\hat{\Theta},\mathfrak{M}} = \prod_{\gamma\in \mathrm{Gal}_k(\boldsymbol{\alpha})\star\theta} (x-\gamma) \in k[x]$$

où $\mathrm{Gal}_k(\boldsymbol{\alpha}) \star \theta = \{\theta^\sigma \mid \sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})\}$ est l'orbite de θ sous l'action du groupe de Galois $\mathrm{Gal}_k(\boldsymbol{\alpha})$ (afin d'alléger la présentation, nous utilisons une notation analogue à celle de l'action d'un ensemble de permutations sur un n-uplet).

THÉORÈME 6. *(Galois). Soit* $\theta \in k(\boldsymbol{\alpha})$. *Alors* $\min_{\theta,k}$, *son polynôme minimal sur k, est celui dont les racines sont les éléments de l'orbite de* θ *sous l'action du groupe de Galois de* $\boldsymbol{\alpha}$ *sur k :*

$$\min_{\theta,k} = \prod_{\gamma\in \mathrm{Gal}_k(\boldsymbol{\alpha})\star\theta} (x-\gamma) = \mathrm{M}_{\hat{\Theta},\mathfrak{M}} \quad .$$

Les éléments θ^σ où σ parcourt le groupe de Galois $\mathrm{Gal}_k(\boldsymbol{\alpha})$ sont appelés les *conjugués* de θ sur k. Ce théorème exprime qu'ils forment l'ensemble des racines du polynôme minimal de θ sur k.

DÉMONSTRATION. Soit $\mathrm{F} := \prod_{\gamma\in \mathrm{Gal}_k(\boldsymbol{\alpha})\star\theta}(x-\gamma)$. Puisque F est la forme sans facteur carré de $\chi_{\hat{\Theta},\mathfrak{M}}$, il appartient à $k[x]$ (toujours vrai sur un corps parfait).
Ce premier fait étant établi, considérons le polynôme $\Theta \in k[x]$ tel que $\Theta(\boldsymbol{\alpha}) = \theta$. Le polynôme $g(\boldsymbol{x}) := \min_{\theta,k}(\Theta)$ appartient à $\mathfrak{M}$ car $g \in k[x]$ et $g(\boldsymbol{\alpha}) = \min_{\theta,k}(\Theta(\boldsymbol{\alpha})) = \min_{\theta,k}(\theta) = 0$. Donc pour toute permutation $\sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})$, $\sigma \cdot g(\boldsymbol{\alpha}) = 0$. Ce qui signifie que pour toute permutation $\sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})$, $0 = \sigma\cdot\min_{\theta,k}(\Theta(\boldsymbol{\alpha})) = \min_{\theta,k}(\sigma\cdot\Theta(\boldsymbol{\alpha})) = \min_{\theta,k}(\theta^\sigma)$; ainsi toute racine de F est racine du polynôme minimal de θ sur k. Donc $\mathrm{F} \in k[x]$ est un facteur du

polynôme minimal de θ sur k. Le polynôme minimal de θ étant celui sur k de moindre degré et de racine θ, il s'identifie à F, unitaire comme lui. □

Exercices. Pour s'habituer à manipuler, montrer que pour tout $\sigma \in S_n$

$$\sigma^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}} = \mathfrak{M}_{\boldsymbol{\alpha}^\sigma} = \mathrm{Id}(\boldsymbol{\alpha}^\sigma) \tag{19}$$

$$\mathrm{Gal}_k(\boldsymbol{\alpha}^\sigma) = \sigma^{-1}\,\mathrm{Gal}_k(\boldsymbol{\alpha})\,\sigma \tag{20}$$

$$\mathrm{V}(\sigma^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}}) = (\mathrm{Gal}_k(\boldsymbol{\alpha})\,\sigma) \star \boldsymbol{\alpha} \quad . \tag{21}$$

On pourra utiliser l'Identité (2). Ces identités traduisent les identités entre idéaux maximaux de relations, leurs variétés et groupes de Galois lorsqu'on change de n-uplet de racines de f.

5. Injecteurs et stabilisateurs d'idéaux

Fixons I, J deux idéaux de $k[x_1, \ldots, x_n]$.

Nous définissons l'*injecteur de* I *dans* J comme étant l'ensemble de permutations qui envoient globalement I dans J :

$$\mathrm{Inj}(\mathrm{I}, \mathrm{J}) := \{\sigma \in S_n \mid \sigma \cdot \mathrm{I} \subset \mathrm{J}\} \quad . \tag{22}$$

Nous avons tout naturellement $\mathrm{Inj}(\mathrm{I}, \mathrm{J}) \cdot \mathrm{I} \subset \mathrm{J}$.

Le *stabilisateur* de l'idéal I est l'ensemble de permutations qui le stabilise globalement :

$$\mathrm{Stab}(\mathrm{I}) := \mathrm{Inj}(\mathrm{I}, \mathrm{I}) \quad .$$

(Dans la littérature, le stabilisateur de I est aussi appelé son *groupe de décomposition* et est noté Dec(I)) .

Comme pour le groupe de Galois, stabilisateur de $\mathfrak{M}$, on montre de la même manière que Stab(I) est un groupe car il est fini, non vide (contient l'identité) et est stable par composition interne. Puisque $\mathrm{Stab}(\mathrm{I}) \cdot \mathrm{I} \subset \mathrm{I}$ et que le stabilisateur est un groupe, nous avons :

$$\mathrm{Stab}(\mathrm{I}) \cdot \mathrm{I} = \mathrm{I} \quad .$$

On peut aussi utiliser l'ordre e de $\sigma \in S_n$. Puisque $\sigma^{-1} = \sigma^{e-1}$ on a $\sigma \cdot \mathrm{I} \subset \mathrm{I} \Rightarrow \mathrm{I} \subset \sigma^{-1} \cdot \mathrm{I} = \sigma \cdot (\sigma^{e-2} \cdot \mathrm{I}) = \sigma \cdot \mathrm{I}$. Donc $\sigma \cdot \mathrm{I} \subset \mathrm{I} \Leftrightarrow \sigma \cdot \mathrm{I} = \mathrm{I}$.

Ou autrement dit :

$$\mathrm{Stab}(\mathrm{I}) = \{\sigma \in \mathrm{S}_n \mid \sigma \cdot \mathrm{I} = \mathrm{I}\} \quad .$$

Comme exemples, nous avons vu : $\mathrm{S}_n = \mathrm{Stab}(\mathfrak{S}) = \mathrm{Inj}(\mathfrak{S}, \mathfrak{M}_{\boldsymbol{\alpha}})$ et $\mathrm{Gal}_k(\boldsymbol{\alpha}) = \mathrm{Stab}(\mathfrak{M}_{\boldsymbol{\alpha}})$.

Ainsi, pour l'idéal des relations symétriques et l'idéal $\mathfrak{M}_{\boldsymbol{\alpha}}$ des α-relations, il y a égalité entre le stabilisateur et l'injecteur dans $\mathfrak{M}_{\boldsymbol{\alpha}}$. Ce ne sera pas toujours le cas pour tous les idéaux dit galoisiens que nous allons définir et étudier, à savoir les idéaux radicaux entre l'idéal des relations symétriques $\mathfrak{S}$ et les idéaux maximaux de relations $\mathfrak{M}$ qui le contiennent. Nous verrons à quelle condition le stabilisateur d'un idéal galoisien s'identifie à son injecteur dans un idéal maximal qui le contient. De tels idéaux galoisiens seront dits *purs*. Nous étudierons leurs propriétés et puis nous les utiliserons pour construire le corps $k(\boldsymbol{\alpha})$ des racines du polynôme f ainsi que le groupe de Galois.

Etudions maintenant quelques relations sur les injecteurs et les stabilisateurs qui nous seront utiles par la suite.

$$\text{Si} \quad \mathrm{I} \subseteq \mathrm{J} \quad \text{alors} \quad \mathrm{Stab}(\mathrm{I}) \subseteq \mathrm{Inj}(\mathrm{I}, \mathrm{J}) \quad . \tag{23}$$

En effet, si $\sigma \in \mathrm{Stab}(\mathrm{I})$ alors $\sigma \cdot \mathrm{I} \subseteq \mathrm{I} \subset \mathrm{J}$. Donc $\sigma \in \mathrm{Inj}(\mathrm{I}, \mathrm{J})$. Comme nous l'avons vu avec l'idéal des relations ou celui des relations symétriques, l'égalité est possible.

$$\text{Si} \quad \mathrm{I} \subseteq \mathrm{I}_1 \quad \text{alors} \quad \mathrm{Inj}(\mathrm{I}_1, \mathrm{J}) \subset \mathrm{Inj}(\mathrm{I}, \mathrm{J}) \quad . \tag{24}$$

En effet, si $\sigma \in \mathrm{S}_n$ alors $\sigma \cdot \mathrm{I}_1 \subset \sigma \cdot \mathrm{I}$ et si $\sigma \in \mathrm{Inj}(\mathrm{I}, \mathrm{J})$ alors $\sigma \cdot \mathrm{I} \subset \mathrm{J}$ d'où $\sigma \cdot \mathrm{I}_1 \subset \mathrm{J}$ et $\sigma \in \mathrm{Inj}(\mathrm{I}_1, \mathrm{J})$.

En particulier, si $\mathrm{I}_1 = \mathrm{J}$ alors $\mathrm{Stab}(\mathrm{J}) \subset \mathrm{Inj}(\mathrm{I}, \mathrm{J})$ et

$$\text{si} \quad \mathrm{I} \subseteq \mathfrak{M}_{\boldsymbol{\alpha}} \quad \text{alors} \quad \mathrm{Gal}_k(\boldsymbol{\alpha}) \subset \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}}) \quad . \tag{25}$$

Soient $\sigma, \tau \in \mathrm{S}_n$ alors :

$$\mathrm{Inj}(\sigma \cdot \mathrm{I}, \tau \cdot \mathrm{J}) = \tau \, \mathrm{Inj}(\mathrm{I}, \mathrm{J}) \, \sigma^{-1} \quad . \tag{26}$$

En effet, par définition de l'injecteur, $\mathrm{Inj}(\sigma \cdot \mathrm{I}, \tau \cdot \mathrm{J}) = \{s \in \mathrm{S}_n \mid s \cdot (\sigma \cdot \mathrm{I}) \subset \tau \cdot \mathrm{J}\}$. D'où

$$\begin{aligned} \mathrm{Inj}(\sigma \cdot \mathrm{I}, \tau \cdot \mathrm{J}) &= \{s \in \mathrm{S}_n \mid \tau^{-1} s \sigma \cdot \mathrm{I} \subset \mathrm{J}\} \\ &= \{\tau t \sigma^{-1} \in \mathrm{S}_n \mid t \cdot \mathrm{I}) \subset \mathrm{J}\} = \tau \, \mathrm{Inj}(\mathrm{I}, \mathrm{J}) \, \sigma^{-1} \end{aligned}$$

en ayant posé $t := \tau^{-1} s \sigma$.

Comme $\mathrm{Stab}(\tau \cdot \mathrm{J}) = \mathrm{Inj}(\tau \cdot \mathrm{J}, \tau \cdot \mathrm{J})$, d'après (26), il vient :

$$\mathrm{Stab}(\tau \cdot \mathrm{J}) = \tau \, \mathrm{Stab}(\mathrm{J}) \, \tau^{-1} \tag{27}$$

Et puisque, d'après l'Identité (19), $\mathrm{Gal}_k(\boldsymbol{\alpha}^\sigma) = \mathrm{Stab}(\sigma^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}})$, nous retrouvons l'Identité (20), à savoir que $\mathrm{Gal}_k(\boldsymbol{\alpha}^\sigma) = \sigma^{-1} \, \mathrm{Gal}_k(\boldsymbol{\alpha}) \, \sigma$.

6. Idéaux galoisiens

Nous allons étudier les idéaux galoisiens généraux. Fixons L un sous-ensemble du groupe symétrique S_n. L'idéal

$$\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}} := \mathrm{Id}_k(\mathrm{L} \star \boldsymbol{\alpha}) \tag{28}$$

est appelé l'*idéal galoisien défini par le couple* $(\mathrm{L}, \boldsymbol{\alpha})$ sur k.

Lorsque L est le groupe identité, nous le notons parfois simplement $\mathrm{I}_{\boldsymbol{\alpha}}$ et nous avons vu précédemment que $\mathfrak{M}_{\boldsymbol{\alpha}} = \mathrm{I}_{\boldsymbol{\alpha}} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{G}_{\boldsymbol{\alpha}}}$.
L'idéal $\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}$ est radical par construction. Nous pouvons l'exprimer également de la manière suivante :

$$\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}} := \{r \in k[\boldsymbol{x}] \mid \forall \sigma \in \mathrm{L} \quad \sigma \cdot r(\boldsymbol{\alpha}) = 0\} \quad .$$

Rappelons que pour $\mathrm{V}_i \subset k^n$, $\mathrm{Id}_k(\mathrm{V}_1 \cup \mathrm{V}_2) = \mathrm{I}_k(\mathrm{V}_1) \cap \mathrm{I}_k(\mathrm{V}_2)$. Pour H_1 et H_2 deux sous-ensembles de S_n, il vient :

$$\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{H}_1} \cap \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{H}_2} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{H}_1 \cup \mathrm{H}_2} \quad .$$

Puisque $\mathrm{L} \star \boldsymbol{\alpha} = \bigcup_{\sigma \in \mathrm{L}} \boldsymbol{\alpha}^\sigma$, nous pouvons encore exprimer notre idéal galoisien sous ces diverses formes :

$$\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}} = \bigcap_{\sigma \in \mathrm{L}} \mathrm{Id}(\boldsymbol{\alpha}^\sigma) = \bigcap_{\sigma \in \mathrm{L}} \sigma^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}} \quad , \tag{29}$$

d'après l'identité (19). Nous pouvons exprimer $\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}$ comme l'intersection d'idéaux comaximaux (voir Section 14). À ce stade, nous n'avons pas encore besoin de cette granularité.

Nous avons toujours $\mathfrak{S} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{S}_n} \subseteq \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}$ et si L contient l'identité, il vient :

$$\mathfrak{S} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{S}_n} \quad \subseteq \quad \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}} \quad \subseteq \quad \mathfrak{M}_{\boldsymbol{\alpha}} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{G}_\alpha} \qquad ,$$

ce qui induit les inclusions inverses suivantes sur les variétés :

$$\mathrm{G}_\alpha \star \boldsymbol{\alpha} \quad \subseteq \quad \mathrm{V}(\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}) \quad \subseteq \quad \mathrm{S}_n \star \boldsymbol{\alpha} \quad .$$

Soit I un idéal galoisien. De par sa définition, l'injecteur $\mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}})$ contient tous les ensembles de permutations L tel que le couple $(\mathrm{L}, \boldsymbol{\alpha})$ définisse I. Ce qui signifie que l'injecteur est leur union :

$$\mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}}) = \{\mathrm{L} \subset \mathrm{S}_n \mid \mathrm{I} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}\} \quad .$$

Variétés galoisiennes

Nous appellerons *galoisienne* la variété algébrique d'un idéal galoisien, i.e. l'ensemble de ses zéros dans $\mathbb{C}$. D'après la proposition suivante, l'ensemble des variétés galoisiennes est formé des ensembles $(\mathrm{Gal}_k(\boldsymbol{\alpha})\,\mathrm{L}) \star \boldsymbol{\alpha}$ où L parcourt les sous-ensembles du groupe symétrique S_n.

PROPOSITION 7. *La variété algébrique et l'injecteur de l'idéal galoisien* I *dans l'idéal maximal* $\mathfrak{M}_{\boldsymbol{\alpha}}$ *sont donnés par :*

$$\mathrm{V}(\mathrm{I}) = \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}}) \star \boldsymbol{\alpha} \quad \textit{avec} \quad \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}}) = \mathrm{Gal}_k(\boldsymbol{\alpha})\mathrm{L} \tag{30}$$

pour tout sous-ensemble L *de* S_n *tel que* $\mathrm{I} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}$ *et où* $\mathrm{GL} := \{g\,l \mid g \in \mathrm{G}\,,\ l \in \mathrm{L}\}$.

DÉMONSTRATION. Posons $\mathrm{I} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}$. D'abord notons que tout élément de V(I) est une permutation de $\boldsymbol{\alpha}$ puisque $\mathrm{V}(\mathrm{I}) \subset \mathrm{S}_n \star \boldsymbol{\alpha} = \mathrm{V}(\mathfrak{S})$. Par définition de l'injecteur $\mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}})$, $\sigma \in \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}})$ si et seulement si pour tout $r \in \mathrm{I}$, $\sigma \cdot r(\boldsymbol{\alpha}) = 0$; ce qui est équivalent à $\boldsymbol{\alpha}^\sigma \in \mathrm{V}(\mathrm{I})$. D'où $\mathrm{V}(\mathrm{I}) = \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}}) \star \boldsymbol{\alpha}$. En utilisant d'abord l'identité (29) puis l'identité (21), il vient :

$$\mathrm{V}(\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}) = \mathrm{V}(\bigcap_{\sigma \in \mathrm{L}} \sigma^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}}) = \bigcup_{\sigma \in \mathrm{L}} \mathrm{V}(\sigma^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}}) = \bigcup_{\sigma \in \mathrm{L}} \mathrm{G}_{\boldsymbol{\alpha}}\sigma \star \boldsymbol{\alpha} = \mathrm{G}_{\boldsymbol{\alpha}}\mathrm{L} \star \boldsymbol{\alpha} \qquad \square$$

REMARQUE 8. D'après (30), pour tout $\sigma \in \mathrm{S}_n$, $\mathrm{V}(\mathrm{Id}_k(\boldsymbol{\alpha}^\sigma)) = \mathrm{V}(\mathrm{I}_{\boldsymbol{\alpha}}^\sigma) = \mathrm{G}_\alpha\sigma \star \boldsymbol{\alpha}$ est la variété algébrique finie associée à l'idéal maximal $\mathrm{Id}_k(\boldsymbol{\alpha}^\sigma)$, donc cet idéal est premier et sa variété est irréductible. Comme l'ensemble des idéaux galoisiens maximaux est formé des $\mathrm{Id}_k(\boldsymbol{\alpha}^\sigma)$ où σ parcourt S_n, toutes les variétés galoisiennes irréductibles sont de la forme $\mathrm{G}_{\boldsymbol{\alpha}}\sigma \star \boldsymbol{\alpha}$.

REMARQUE 9. Il est possible de démontrer la proposition précédente d'une autre manière en considérant un polynôme $\Theta \in k[\boldsymbol{x}]$ tel que $\mathrm{L} = \mathrm{Stab}_{\mathrm{S}_n}(\Theta)$, dit L-*invariant* (*primitif*), et tel que si $\sigma \cdot \Theta(\boldsymbol{\alpha}) = \Theta(\boldsymbol{\alpha})$ alors $\sigma \in \mathrm{L}$; le polynôme Θ est appelé un L-*invariant* $\boldsymbol{\alpha}$-*séparable*. Ensuite, il suffit de constater que $g(\Theta) \in \mathrm{I}$, où $g(x)$ est le polynôme caractéristique $\chi_{\Theta,\mathrm{I}}(x)$.

COROLLAIRE 10. *Les variétés galoisiennes irréductibles contenues dans* $\mathrm{V}(\mathrm{I})$ *sont les variétés* $(\mathrm{Gal}_k(\boldsymbol{\alpha})\sigma) \star \boldsymbol{\alpha}$ *où* σ *parcourt tout sous-ensemble* L *tel que* $\mathrm{I} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}$ *; ce qui en particulier est le cas pour* $\mathrm{L} = \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}})$.

Posons $\mathrm{I} := \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}$.

LEMME 11. *Soit* $\boldsymbol{\alpha}$ *un* n*-uplet des racines (distinctes) du polynôme* f*. L'ensemble des idéaux maximaux contenant* I *est formé des* $\sigma^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}}$ *où* σ *parcourt* $\mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}})$.

DÉMONSTRATION. Nous avons, $\mathrm{V}(\mathrm{I}) = \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}}) \star \boldsymbol{\alpha}$ et $\mathrm{I} = \mathrm{Id}(\mathrm{V}(\mathrm{I}))$ qui est donc l'intersection des idéaux maximaux $\mathrm{Id}(\boldsymbol{\alpha}^{\sigma})$ où σ parcourt $\mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}})$. Donc si $\mathfrak{M}$ est un idéal maximal contenant I alors il est nécessairement de la forme $\mathrm{Id}(\boldsymbol{\alpha}^{\sigma})$ où $\sigma \in \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}})$. Or, d'après l'identité (19), nous avons $\mathfrak{M} = \mathrm{Id}(\boldsymbol{\alpha}^{\sigma}) = \sigma^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}}$. Ce qui achève la preuve. □

Puisque la Proposition 30 donne la variété de I et que I est radical, pour tout polynôme $\Theta \in k[\boldsymbol{x}]$ nous pouvons exprimer le polynôme caractéristique $\chi_{\hat{\Theta},\mathrm{I}}$ de $\hat{\Theta}$, l'endomorphisme multiplicatif de $k[\boldsymbol{x}]/\mathrm{I}$ induit par Θ :

$$\chi_{\hat{\Theta},\mathrm{I}}(x) = \prod_{\boldsymbol{\beta} \in \mathrm{V}(\mathrm{I})} (x - \Theta(\boldsymbol{\beta})) = \prod_{\sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})\mathrm{L}} (x - \sigma \cdot \Theta(\boldsymbol{\alpha})) \quad \in k[x] \qquad . \tag{31}$$

Cette formule du polynôme caractéristique généralise ce que nous avons vu avec l'idéal maximal $\mathfrak{M}_{\boldsymbol{\alpha}}$. Le produit s'étend à seulement L lorsque L est un groupe contenant $\mathrm{Gal}_k(\boldsymbol{\alpha})$. Nous étudierons plus loin les idéaux galoisiens dits "purs" ayant cette propriété.

Correspondance galoisienne des idéaux galoisiens

Nous déduisons des résultats précédents les **correspondances galoisiennes** sur les idéaux galoisiens.

Soient deux idéaux galoisiens I et J tels que

$$\mathfrak{S} \subsetneq \mathrm{I} \subsetneq \mathrm{J} \subsetneq \mathfrak{M}_{\boldsymbol{\alpha}} \quad ,$$

alors nous avons les inclusions inverses suivantes sur leurs injecteurs :

$$S_n = \mathrm{Stab}(\mathfrak{S}) \quad \supsetneq \quad \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}}) \quad \supsetneq \quad \mathrm{Inj}(J, \mathfrak{M}_{\boldsymbol{\alpha}}) \quad \supsetneq \quad \mathrm{Stab}(\mathfrak{M}_{\boldsymbol{\alpha}}) = G_{\boldsymbol{\alpha}} \quad .$$

Inversement, soient L et H deux sous-ensembles (pas nécessairement sous-groupes) de S_n tels que :

$$S_n \quad \supsetneq \quad L \quad \supsetneq H$$

alors

$$\mathfrak{S} \quad \subseteq \quad I_{\boldsymbol{\alpha}}^{L} \quad \subseteq \quad I_{\boldsymbol{\alpha}}^{H} \quad .$$

Il peut y avoir égalité, comme en particulier lorsque $G_{\boldsymbol{\alpha}} = S_n$: dans ce cas, tous les idéaux galoisiens sont identiques à l'idéal $\mathfrak{S}$ des relations symétriques.

Si, de plus, $\boldsymbol{\alpha} \in V(I_{\boldsymbol{\alpha}}^{H})$ (i.e. si L et H contiennent l'identité) alors

$$\mathfrak{S} \quad \subseteq \quad I_{\boldsymbol{\alpha}}^{L} \quad \subseteq \quad I_{\boldsymbol{\alpha}}^{H} \quad \subseteq \quad \mathfrak{M}_{\boldsymbol{\alpha}} \quad .$$

Notons que $H \subseteq G_{\boldsymbol{\alpha}}$ si et seulement si $I_{\boldsymbol{\alpha}}^{H} = \mathfrak{M}_{\boldsymbol{\alpha}}$.

Les inégalités sur les variétés galoisiennes s'en suivent puisque chaque variété d'un idéal galoisien I est de la forme $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}^\sigma}) \star \boldsymbol{\alpha}^\sigma$, c'est-à-dire est l'orbite d'un n-uplet des racines de f par l'injecteur de I dans l'idéal (maximal) de ce point.

REMARQUE 12. Pour ceux ayant étudié la correspondance galoisienne sur les corps, ils se souviennent qu'il y a une correspondance bijective entre les sous-groupes du groupe de Galois G de f sur k et les corps intermédiaires entre le corps $k = k(\boldsymbol{\alpha})^G$ et le corps $k(\boldsymbol{\alpha}) \simeq k[\boldsymbol{x}]/\mathfrak{M}_{\boldsymbol{\alpha}}$. Ici, c'est "un peu" le contraire. Tous les sous-ensembles (non nécessairement des groupes) du groupe de Galois $G_{\boldsymbol{\alpha}}$ définissent le même idéal galoisien $\mathfrak{M}_{\boldsymbol{\alpha}}$ (maximal) et ce sont les ensembles L entre S_n et le groupe de Galois $G_{\boldsymbol{\alpha}}$ qui définissent tous les idéaux galoisiens $\mathrm{Id}_k(L \star \boldsymbol{\alpha})$ compris entre $\mathrm{Id}_k(S_n \star \boldsymbol{\alpha})$ et $\mathrm{Id}_k(G_{\boldsymbol{\alpha}} \star \boldsymbol{\alpha}) = \mathfrak{M}_{\boldsymbol{\alpha}}$.

7. Idéaux galoisiens purs

Nous fixons un idéal galoisien $I := I_{\boldsymbol{\alpha}}^{L} = \mathrm{Id}_k(L \star \boldsymbol{\alpha})$ où L est un sous-ensemble de S_n. Rappelons que $\mathfrak{M}_{\boldsymbol{\alpha}} = \mathrm{Id}_k(\boldsymbol{\alpha}) = I_{\boldsymbol{\alpha}}$.

Nous nous intéressons ici au cas dans lequel l'injecteur $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$ est un groupe : comment le vérifier et quelles en sont les conséquences ?

D'abord lorsque L contient l'identité, nous pouvons appliquer le lemme suivant :

LEMME 13. *Si* $I \subseteq \mathfrak{M}_{\boldsymbol{\alpha}}$ *alors* $\mathrm{Stab}(I)$ *contient tous les sous-groupes* H *du groupe symétrique* S_n *tels que* $I = I_{\boldsymbol{\alpha}}^{H}$.

DÉMONSTRATION. Soit H un sous-groupe de S_n tel que $I = I_{\boldsymbol{\alpha}}^H$. Prenons $h \in H$ et $r \in I$. Nous savons que $h \cdot r \in I$ est équivalent à $\sigma \cdot (h \cdot r)(\boldsymbol{\alpha}) = 0$ pour tout $\sigma \in H$, par définition de $I_{\boldsymbol{\alpha}}^H$. Or puisque H est un groupe, $\sigma h \in H$ et, par conséquent, par définition de $I_{\boldsymbol{\alpha}}^H$, $0 = \sigma h \cdot r(\boldsymbol{\alpha}) = \sigma \cdot (h \cdot r)(\boldsymbol{\alpha})$. Donc $h \cdot r \in I$ et $h \in \mathrm{Stab}(I)$. □

THÉORÈME 14. *Soit* I *un idéal galoisien de* f *sur* k *et* $\boldsymbol{\alpha}$ *un* n*-uplet de racines (distinctes) du polynôme* f *de* $k[x]$. *L'injecteur* $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$ *est un groupe si et seulement si il existe un sous-groupe* L *de* S_n *qui contient le groupe de Galois* $G_{\boldsymbol{\alpha}}$ *et tel que* $I = \mathrm{Id}(L \star \boldsymbol{\alpha})$.

DÉMONSTRATION. Montrons la condition suffisante. Si L est un sous-groupe de S_n qui contient $G_{\boldsymbol{\alpha}}$ avec $I = \mathrm{Id}(L \star \boldsymbol{\alpha})$ alors $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}}) = G_{\boldsymbol{\alpha}} L = L$ est un groupe. Inversement, supposons que l'injecteur $L := \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$ soit un groupe. Puisque L contient l'identité, nous avons $I \subseteq \mathfrak{M}_{\boldsymbol{\alpha}}$. Nous en déduisons l'inclusion inverse sur leurs injecteurs : $G_{\boldsymbol{\alpha}} = \mathrm{Stab}(G_\alpha) \subseteq \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}}) = L$.De plus, par définition de l'injecteur, $(L, \boldsymbol{\alpha})$ définit l'idéal I : $I = \mathrm{Id}(L \star \boldsymbol{\alpha})$ (c'est même le plus grand ensemble de permutations qui définisse I). La réciproque est prouvée. □

D'après le théorème précédent, nous constatons que si $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$ est un groupe alors c'est le groupe L du théorème qui contient le groupe de Galois puisque $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}}) = G_{\boldsymbol{\alpha}} L = L$.

THÉORÈME 15. *Soit un polynôme* f *de* $k[x]$ *sans racines multiple, de degré* n *et* $\boldsymbol{\alpha}$ *un* n*-uplet de ses racines. Soit* I *un idéal galoisien de* f *sur* k. *Si* $\boldsymbol{\alpha} \in V(I)$ *alors :*
(i) si l'injecteur $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$ *est un groupe alors pour tout idéal maximal* $\mathfrak{M}$ *contenant* I, *il y a l'identité* $\mathrm{Stab}(I) = \mathrm{Inj}(I, \mathfrak{M})$ *et c'est en particulier le cas pour* $\mathfrak{M} = \mathfrak{M}_{\boldsymbol{\alpha}}$ *;*
(ii) s'il existe un idéal maximal $\mathfrak{M}$ *tel que* $\mathrm{Stab}(I) = \mathrm{Inj}(I, \mathfrak{M})$ *alors* $I \subset \mathfrak{M}$ *et* $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$ *est lui aussi le groupe* $\mathrm{Stab}(I)$.

DÉMONSTRATION. Supposons que l'injecteur L de I dans un idéal maximal $\mathfrak{M}_{\boldsymbol{\alpha}}$ soit un groupe (il ne pourrait pas l'être si $\alpha \notin V(I)$). Nous avons $I = I_{\boldsymbol{\alpha}}^L \subseteq I_{\boldsymbol{\alpha}}$ puisque L contient l'identité. Par conséquent, $L \subseteq \mathrm{Stab}(I)$, d'après le lemme 13. Or, d'après l'identité (23), $\mathrm{Stab}(I) \subseteq \mathrm{Inj}(I, J)$ si $I \subseteq J$. Donc en appliquant ceci à $J = \mathfrak{M}_{\boldsymbol{\alpha}}$, nous obtenons l'inclusion inverse et nous avons montré que $\mathrm{Stab}(I) = \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$.
Soit maintenant $\mathfrak{M}$ un idéal maximal quelconque contenant I. Alors il existe $\tau \in \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$ tel que $\mathfrak{M} = \tau^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}}$ (voir Lemme 11 sur l'ensemble des idéaux maximaux contenant I). Ainsi, d'après l'identité (26), $\mathrm{Inj}(I, \mathfrak{M}) = \tau^{-1} \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}}) = \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$ puisque $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$ est un groupe. Et donc tout comme pour $\mathfrak{M}_{\boldsymbol{\alpha}}$, nous avons $\mathrm{Inj}(I, \mathfrak{M}) = \mathrm{Stab}(I)$. □

Autrement dit, l'injecteur d'un idéal galoisien I dans un idéal maximal $\mathfrak{M}$ est un groupe si et seulement si pour un élément quelconque $\boldsymbol{\alpha}$ de la variété irréductible $V(\mathfrak{M})$, il existe un groupe L qui contienne $\mathrm{Stab}(\mathfrak{M}) = G_{\boldsymbol{\alpha}}$ et tel que l'idéal $I = Id_k(L \star \boldsymbol{\alpha})$. Dans

ce cas, le groupe L est à la fois le stabilisateur de I et l'injecteur de I dans $\mathfrak{M}'$ pour tout idéal maximal $\mathfrak{M}'$ contenant de I (i.e. tous ces injecteurs sont égaux au groupe stabilisateur). Un tel idéal galoisien est appelé un idéal galoisien *pur*.

Lorsque qu'un idéal galoisien I est pur, nous avons pour tout $\boldsymbol{\beta} \in \mathrm{V(I)}$:

$$\mathrm{V(I)} = \mathrm{Stab(I)} \star \boldsymbol{\beta} = \{(\beta_{\sigma(1)}, \ldots, \beta_{\sigma(n)}) \mid \sigma \in \mathrm{Stab(I)}\} \quad .$$

En effet, soit $\boldsymbol{\beta} \in \mathrm{V(I)}$. Puisque I est pur, nous avons $\mathrm{Inj(I}, \mathfrak{M}_{\boldsymbol{\beta}}) = \mathrm{Stab(I)}$ et donc $\mathrm{V(I)} = \mathrm{Stab(I)} \star \boldsymbol{\beta}$, d'après la proposition 7.

Ainsi, pour tout polynôme $\Theta \in k[\boldsymbol{x}]$, lorsque I est galoisien pur :

$$\chi_{\hat{\Theta},\mathrm{I}}(x) = \prod_{\boldsymbol{\beta} \in \mathrm{V(I)}} (x - \Theta(\boldsymbol{\beta})) = \prod_{\sigma \in \mathrm{Stab(I)}} (x - \sigma \cdot \Theta(\boldsymbol{\alpha})) \in k[x] \quad . \tag{32}$$

Alors que le calcul d'un injecteur dans un idéal maximal contenant I nécessite d'avoir déterminé le groupe de Galois, dans le cas des idéaux galoisiens purs, comme cet injecteur s'identifie au stabilisateur de I, ce calcul devient réalisable sans le groupe de Galois. En effet, nous verrons comment que le stabilisateur d'un idéal galoisien pur se calcule rapidement à partir d'un certain ensemble de ses générateurs.

COURS 12

8. Complément sur les générateurs d'un idéal galoisien pur

Nous supposons que I est un idéal galoisien pur de stabilisateur L = Stab(I). Puisqu'il est pur, l'idéal I est triangulaire (voir Théorème cours 11). Fixons

$$\{f_1(x_1,\dots,x_n),\dots,f_{n-1}(x_{n-1},x_n),f_n(x_n)\}$$

un ensemble triangulaire séparable engendrant I et posons $d_s = \deg_{x_s} f_s$.

Nous pouvons choisir ces générateurs de I de telle sorte que $\deg_{x_j} f_s < d_j$ si $j \neq s$; l'ensemble triangulaire est alors dit *réduit*; c'est toujours possible d'obtenir un ensemble triangulaire "réduit" à partir d'un qui ne l'est pas en divisant (réduisant) les générateurs les uns avec les autres selon la variable la plus forte suivant cet ordre sur les variables : $x_1 > \cdots > x_n$.

Notons que $d_1 = 1$. En fait $f_1 = x_1 + \cdots + x_n - b$ où b est la sommes $\alpha_1 + \ldots + \alpha_n$ des racines, opposée au coefficient sous-dominant dans l'expression du polynôme f (i.e. de x^{n-1}).

Considérons la suite $(\mathrm{L}_r)_{r\in[\![1,n+1]\!]}$ de sous-groupes définie inductivement ainsi : $\mathrm{L}_{n+1} :=$ L et $\mathrm{L}_r := \{\sigma \in \mathrm{L}_{r+1} \mid \sigma(r) = r\}$ pour $r \in [\![1,n]\!]$. Pour tout $\boldsymbol{\alpha} \in \mathrm{V(I)}$, comme nous l'avions fait pour les modules de Cauchy, nous considérons $\mathrm{F}_n(x_n) := f_n(x_n)$ et pour chaque $r \in [\![1,n-1]\!]$:

(33) $\mathrm{F}_r(\boldsymbol{x}_r) := f_r(\boldsymbol{x}_r,\alpha_{r+1},\dots,\alpha_{n-1},\alpha_n) = (\boldsymbol{x}_r - \alpha_{\sigma_1(r)})(\boldsymbol{x}_r - \alpha_{\sigma_2(r)})\cdots(\boldsymbol{x}_r - \alpha_{\sigma_{d_r}(r)})$

où l'ensemble $\mathrm{T}_r := \{\sigma_1,\dots,\sigma_{d_r}\}$ est une transversale à gauche de $\mathrm{L}_{r+1} \mod \mathrm{L}_r$ de cardinal $d_r = \deg_{x_r} f_r$ avec $\sigma_{d_r} = id$:

$$\mathrm{L}_{r+1} = \sigma_1\mathrm{L}_r + \cdots + \sigma_{d_r}\mathrm{L}_r \quad .$$

Par exemple, $\mathrm{L}_n = \{\sigma \in \mathrm{L} \mid \sigma(n) = n\}$. Si le groupe L est transitif alors $\mathrm{F}_n(x_n) = f_n(x_n) = (x_n - \alpha_1)\cdots(x_n - \alpha_n)$.

Chaque polynôme $\mathrm{F}_r(\boldsymbol{x}_r)$, $r \in [\![1,n-1]\!]$, dépend de l'ensemble $\{\mathrm{F}_{r+1}(x_{r+1}),\dots,\mathrm{F}_n(x_n)$ de polynômes et du choix d'un leurs zeros $(\alpha_{r+1},\dots,\alpha_n)$ dans $\overline{k}^{n-r}$. Pour des raisons de lisibilité, nous évitons de le notifier, tout en considérant que ce sera contextuel.

REMARQUE 16. Si H est un groupe alors la transversale de $\mathrm{H} \mod \mathrm{Stab}_{\mathrm{H}}(r)$ est appelée aussi la *transversale de r dans* H.
Par exemple, le logiciel libre `SageMath` (téléchargement et compte en ligne `Cocalc` gratuits) la calcule avec la commande `H.transversale(r)`. De même `H.stabiliser(r)` calcule $\mathrm{Stab}_{\mathrm{H}}(r)$.

Nous disposons donc de tous les moyens pour décrire un idéal galoisien pur à partir de son stabilisateur.

REMARQUE 17. Lorsque $\mathrm{I} = \mathfrak{M}_{\boldsymbol{\alpha}}$, $\mathrm{L} = \mathrm{Gal}_k(\boldsymbol{\alpha})$, les polynômes f_r sont les modules fondamentaux $\mathfrak{F}_r$ et $\mathrm{F}_r(x_r) = \mathfrak{F}_r(x_r, \alpha_{r+1}, \ldots, \alpha_{n-1}, \alpha_n) = \min_{\alpha_r,k}(x_r)$. Des résultats généraux précédents sur les idéaux galoisiens purs, nous pouvons donc déduire des propriétés sur des sous-corps du corps de décomposition $k(\boldsymbol{\alpha})$ et des sous-groupes du groupe de Galois.

9. Réduction par un idéal triangulaire (Rappel)

Nous supposons que I est un triangulaire engendré par

$$\{f_1(x_1, \ldots, x_n), \ldots, f_{n-1}(x_{n-1}, x_n), f_n(x_n)\}$$

un ensemble triangulaire séparable. Posons $d_s = \deg_{x_s} f_s$.

Fixons maintenant un polynôme $p \in k[\boldsymbol{x}]$. Sa classe $[p]$ dans $k[\boldsymbol{x}]/\mathrm{I}$ possède un unique représentant dans la base $\mathscr{B}$ monomiale de $k[\boldsymbol{x}]/\mathrm{I}$ formée des monômes :

$$x_1^{i_1} \ldots x_n^{i_n} \quad \text{où} \quad 0 \leq i_s < d_s$$

(voir Cours-TDs précédents). On retrouve que le cardinal de la variété de I est $d = d_1 \cdots d_n = \#\mathrm{L}$ car les racines de f sont deux-à-deux distinctes. Ce représentant $[p]$ est obtenu par une opération de **réduction dite "modulo I"** qui, dans le cas des idéaux galoisiens purs, consiste en les n divisions euclidiennes successives suivantes :

posons $p_1 := p$ et définissons récursivement les polynômes $p_2, \ldots, p_{n+1}$ comme suit :

$$p_r(x_1, \ldots, \mathbf{x_r}, \ldots, x_n) = \$ f_r(\mathbf{x_r}, \ldots, x_n) + p_{r+1}(\boldsymbol{x})$$

où $p_{r+1}(\boldsymbol{x})$ est le reste de la division euclidienne de p_r par f_r en x_r pour $r \in [\![1, n]\!]$. Le dernier reste p_{n+1} est, par construction, une combinaison linéaire de monômes de la base $\mathscr{B}$. Il est donc le représentant unique de $[p]$ dans cette base.

10. Tester par le calcul qu'un idéal galoisien est ou non pur

Nous sommes en mesure de tester si un idéal galoisien J est pur ou ne l'est pas. Nous supposons ne disposer que d'un système de générateurs de J. Nous devons supposer savoir tester si un idéal est triangulaire ou non et s'il l'est, nous devons pouvoir disposer de l'ensemble triangulaire séparable qui l'engendre.

Si J n'est pas triangulaire, alors il n'est pas pur. Si J est triangulaire, pour qu'il soit pur, il faut et il suffit que pour un idéal maximal $\mathfrak{M}$ quelconque contenant J, l'injecteur de J dans $\mathfrak{M}$ et Stab(J) soient identiques. Il suffit donc de tester si leurs cardinaux sont ou non égaux puisque Stab(J) est nécessairement inclus dans cet injecteur.

L'injecteur de J n'est pas directement calculable sans $\mathfrak{M}$, ou plutôt sans son stabilisateur Stab($\mathfrak{M}$), groupe de Galois. de tout $\boldsymbol{\alpha} \in V(\mathfrak{M})$. Pour autant, son cardinal est celui de la variété de J (car les racines de f sont deux-à-deux distinctes), lui-même identique au produit d des degré initiaux des polynômes de l'ensemble triangulaire qui engendre J.

En revanche, il est facile de tester si un groupe G est ou non identique à Stab(I) : il suffit de tester l'appartenance à I des permutés des générateurs de I par ceux de G. Il suffit de faire le test sur des groupes d'ordre inférieur à d. En particulier, le stabilisateur d'un idéal triangulaire I est calculable à partir de l'ensemble triangulaire qui l'engendre (nous savons le faire dans des cas plus généraux mais cela sort du cadre de ce cours).

Voici un algorithme simple qui teste la pureté d'un idéal galoisien triangulaire J $=< f_1, \ldots, f_n >$, $f_i \in k[x_i, \ldots, x_n]$, tout en déterminant son stabilisateur quand il est pur :

(1) Calculer d, le cardinal de l'injecteur de J dans $\mathfrak{M}$, un idéal maximal quelconque : $d = \prod_{i=1}^{n} deg_{x_i}(f_i)$

(2) Chercher Stab(J) parmi les groupes d'ordre d et possiblement candidats

(3) Si Stab(J) est parmi les groupes de cardinal d alors J est pur sinon il ne l'est pas.

Exo Pouvez-vous proposer un test plus efficace qui utiliserait des pré-calculs sur les groupes ?

11. Du Théorème fondamental des fonctions symétriques au théorème de Galois

Il s'agit d'évaluer en les racines de f.

L'effectivité du théorème fondamental des fonctions symétriques consiste à trouver la valeur dans k d'un polynôme symétrique s évalué en les racines de f (pouvant être éventuellement le polynôme $(x - x_1) \cdots (x - x_n)$). Celui de Galois, consiste à prendre un polynôme p invariant par le groupe de Galois $G_{\boldsymbol{\alpha}}$ et de calculer $p(\boldsymbol{\alpha})$. Nous avons vu que $s(\boldsymbol{\alpha})$ et $p(\boldsymbol{\alpha})$ s'obtiennent en réduisant respectivement s modulo l'idéal des relations symétriques $\mathfrak{S}$ et p modulo l'idéal maximal des $\boldsymbol{\alpha}$-relations $\mathfrak{M}_{\boldsymbol{\alpha}}$. Il s'agit en fait d'un même théorème qui se généralise à tout idéal galoisien pur ou non. Pour ce cours, nous en resterons aux idéaux galoisiens purs :

THÉORÈME 18. *Soit p un polynôme invariant par le stabilisateur d'un idéal galoisien pur* I. *Alors pour tout $\boldsymbol{\alpha} \in$ I, $p(\boldsymbol{\alpha}) \in k$ et $p(\boldsymbol{\alpha})$ s'obtient par la réduction de p modulo* I, *soit par n divisions successives avec les n polynômes triangulaires engendrant* I.

DÉMONSTRATION. il suffit de constater que $p(\boldsymbol{\alpha}) \in k$ car p est invariant par le stabilisateur Stab(I) qui contient le groupe de Galois $G_{\boldsymbol{\alpha}}$ puisque I est pur. Ainsi $q := p - p(\boldsymbol{\alpha}) \in I$ puisque pour tout $\sigma \in \text{Stab(I)}$, $\sigma \cdot q(\boldsymbol{\alpha}) = q(\boldsymbol{\alpha}) = 0$. □

12. Polynôme caractéristique et résolvante

Nous fixons un idéal galoisien $I := I^L_{\boldsymbol{\alpha}}$ et $\Theta \in k[\boldsymbol{x}]$.

12.1. Polynôme caractéristique. Nous considérons l'endomorphisme multiplicatif $\hat{\Theta}$ induit par Θ dans $k[\boldsymbol{x}]/I$. Le polynôme caractéristique de $\hat{\Theta}$ est donné par :

$$\begin{aligned} \chi_{\Theta,I}(x) &= \prod_{\boldsymbol{\beta} \in V(I)} (x - \Theta(\boldsymbol{\beta})) \\ &= \prod_{\sigma \in \text{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})} (x - \sigma.\Theta(\boldsymbol{\alpha})) \quad , \end{aligned} \tag{34}$$

d'abord car tout idéal galoisien est radical et ensuite d'après l'identité (30) : V(I) = $\text{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}}) \star \boldsymbol{\alpha}$ (voir partie de Cours de Fabrice Rouillier qui exprime le polynôme caractéristique à partir de la variété de I et qui montre que lorsque l'idéal I est radical, les multiplicités des zéros sont toutes identiques à 1).

REMARQUE 19. Puisque l'idéal I est radical et le corps k parfait, le polynôme minimal $M_{\Theta,I}$ de $\hat{\Theta}$ est la forme sans facteur carré du polynôme caractéristique $\chi_{\Theta,I}$. (Exercice).

Rappel : calcul du polynôme caractéristique avec des résultants (traité par Philippe Aubry)

Nous présentons une méthode inspirée de Lagrange pour calculer sa résolvante que nous définirons plus loin :

THÉORÈME 20. *Posons* $g_0 := y - \Theta(\boldsymbol{x})$, $g_r(x_1, \ldots, x_{n-r}) := \text{Res}_{x_r}(f_r, g_{r-1})$ *pour* $r \in [[1, n-1]]$ *et* $g_n := \text{Res}_{x_n}(f_n, g_{n-1}) \in k[y]$.
Alors le polynôme caractéristique est donné par : $\chi_{\Theta,I} = g_n$. *Nous pouvons écrire cela ainsi :*

$$\chi_{\Theta,I}(y) = \text{Res}_{x_n}(f_n, \text{Res}_{x_{n-1}}(f_{n-1}, \ldots, \text{Res}_{x_2}(f_2, \text{Res}_{x_1}(f_1, y - \Theta)) \cdots)) \quad .$$

Notons que $\text{Res}_{x_1}(f_1(\boldsymbol{x}), x - \Theta(\boldsymbol{x})) = x - \Theta(b - x_2 - \cdots - x_n, x_2, \ldots, x_n)$ puisque $f_1 = x_1 + \cdots + x_n - b$. Notons encore que si g_{r-1} ne dépend pas de x_r alors on posera $g_r = g_{r-1}$ pour éviter de calculer un résultant qui retournerait $g_{r-1}^{d_r}$. Pour optimiser les calculs, à chaque étape, il faudra réduire le polynôme g_r modulo $< f_1, \ldots, f_{r-1} >$. Si des résultants inutiles sont évités, le polynôme caractéristique sera alors une puissance du polynôme

g_n ainsi obtenu. Il existe une méthode optimisée pour calculer ainsi le polynôme caractéristique en réduisant les calculs tout en évitant certains inutiles. Elle sort du cadre de ce cours.

Nous pouvons maintenant prouver notre théorème.

DÉMONSTRATION. Pour démontrer, il faut faire le chemin inverse de celui du calcul qui commence par g_1 pour finir à g_n. Nous allons utiliser la notation simplifiée (33) avec les polynômes F_i. Puisque F_n est unitaire, nous avons

$$g_n = \mathrm{Res}_{x_n}(f_n, g_{n-1}) = \prod_{\mathrm{F}_n(\alpha_n)=0} g_{n-1}(\alpha_n)$$

où le produit sur les racines de F_n comptées avec leurs multiplicités (car c'est un résultant) peut s'écrire ainsi car $\mathrm{F}_n = f_n$ est sans racine multiple. Ensuite, pour toute racine α_n de F_n, puisque F_n est unitaire, nous avons

$$g_{n-1}(\alpha_n) = \mathrm{Res}_{x_{n-1}}(\mathrm{F}_{n-1}, g_{n-2}(x_{n-1}, \alpha_n)) = \prod_{\mathrm{F}_{n-1}(\alpha_{n-1})=0} g_{n-2}(\alpha_{n-1}, \alpha_n)$$

où le produit sur toutes les racines de F_{n-1} comptées avec leurs multiplicités peut s'écrire ainsi car F_{n-1} est sans racine multiple. En poursuivant, nous aboutissons naturellement à

$$g_n = \prod_{\mathrm{F}_n(\alpha_n)=0} \prod_{\mathrm{F}_{n-1}(\alpha_{n-1})=0} \cdots \prod_{\mathrm{F}_2(\alpha_2)=0} \prod_{\mathrm{F}_1(\alpha_1)=0} (y - \Theta(\alpha_1, \ldots, \alpha_n))$$

qui correspond bien au polynôme caractéristique puisque les racines sont les $\Theta(\alpha_1, \ldots, \alpha_n)$ où $(\alpha_1, \ldots, \alpha_n)$ parcourt $\mathrm{V}(\mathrm{I})$. □

Le polynôme caractéristique peut s'avérer coûteux à calculer en raison de son degré. En effet, pour $\mathrm{L} := \mathrm{S}_n$, il sera de degré $n!$. Quand au polynôme minimal $\mathrm{M}_{\Theta,\mathrm{I}}$ de l'endomorphisme multiplicatif $\hat{\Theta}$, la forme sans facteur carré de $\chi_{\Theta,\mathrm{I}}$ (car k est parfait et I radical), il ne peut être calculé directement dans l'ignorance du groupe de Galois $\mathrm{G}_{\boldsymbol{\alpha}}$.

Nous avons donc recours à l'outil algébrique puissant et intermédiaire qu'est la *résolvante* introduite par Lagrange dans le cas $\mathrm{L} := \mathrm{S}_n$.

12.2. La résolvante. Rappelons que pour $\mathrm{L} \subset \mathrm{S}_n$, l'ensemble $\mathrm{L}\cdot\Theta = \{\Theta(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \mid \sigma \in \mathrm{L}\}$ est l'orbite du polynôme Θ sous l'action de L.

Le polynôme unitaire et univarié

$$\mathrm{R}_{\Theta,\mathrm{I},\boldsymbol{\alpha}} = \prod_{\Psi \in \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}})\cdot\Theta} (x - \Psi(\boldsymbol{\alpha}))$$

est indépendant du choix de $\boldsymbol{\alpha}$ dans $\mathrm{V}(\mathfrak{S})$ (i.e. du n-uplet quelconque de racines de f choisi).

DÉMONSTRATION. Soit $\boldsymbol{\beta} = \boldsymbol{\alpha}^\sigma$, où $\sigma \in S_n$. On a $\mathfrak{M}_{\boldsymbol{\beta}} = \sigma^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}}$, d'après l'Identité (19). Puisque $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\beta}}) = \sigma^{-1}\,\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$, d'après (26), l'appartenance : $\Psi \in \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\beta}}) \cdot \Theta$ est alors équivalente à la suivante : $\sigma \cdot \Psi \in \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}}) \cdot \Theta$. Ainsi

$$\begin{aligned} R_{\Theta,I,\boldsymbol{\beta}} &= \prod_{\Psi \in \sigma^{-1}\,\mathrm{Inj}(I,\mathfrak{M}_{\boldsymbol{\alpha}})\cdot\Theta} (x - \Psi(\boldsymbol{\beta})) \\ &= \prod_{\sigma\cdot\Psi \in \mathrm{Inj}(I,\mathfrak{M}_{\boldsymbol{\alpha}})\cdot\Theta} (x - \Psi(\boldsymbol{\alpha}^\sigma)) \quad . \end{aligned}$$

Pour finir, en posant $L := \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$ et $\Psi' := \sigma \cdot \Psi$, nous obtenons $R_{\Theta,I,\boldsymbol{\beta}} = \prod_{\Psi' \in L\cdot\Theta}(x - \sigma^{-1} \cdot \Psi'(\boldsymbol{\alpha}^\sigma)) = R_{\Theta,I,\boldsymbol{\alpha}}$ puisque $\sigma^{-1} \cdot \Psi'(\boldsymbol{\alpha}^\sigma) = \Psi'(\boldsymbol{\alpha})$. □

Nous définissons la *résolvante* de I par Θ comme le polynôme univarié suivant :

$$R_{\Theta,I} = \prod_{\Psi \in \mathrm{Inj}(I,\mathfrak{M}_{\boldsymbol{\alpha}})\cdot\Theta} (x - \Psi(\boldsymbol{\alpha})) \in k[x] \quad , \quad \forall \boldsymbol{\alpha} \in V(\mathfrak{S}) \tag{35}$$

qui ne dépend pas du choix de $\boldsymbol{\alpha}$ parmi les n-uplets de racines (distinctes) du polynôme univarié f de $k[x]$.

Il y a plusieurs façons de prouver que les coefficients de $R_{\Theta,I}$ appartiennent effectivement à k. La plus rapide est de choisir $\boldsymbol{\alpha} \in V(I)$; i.e. $I \subset \mathfrak{M}_{\boldsymbol{\alpha}}$. Comme alors $G_{\boldsymbol{\alpha}} = \mathrm{Inj}(\mathfrak{M}_{\boldsymbol{\alpha}}, \mathfrak{M}_{\boldsymbol{\alpha}}) \subseteq \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$ (voir Identité (24)), les coefficients de la résolvante sont invariants par le groupe de Galois $G_{\boldsymbol{\alpha}}$ (car résultent de fonctions symétriques de $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})\cdot\Theta$ et $G_{\boldsymbol{\alpha}} \subset \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$). On conclut alors par le Théorème de Galois.

La résolvante de Lagrange notée $R_{\Theta,f}$ est celle associée à l'idéal des relations symétriques. Elle ne dépend pas de l'ordre des racines et s'exprime sous cette forme :

$$R_{\Theta,f} = \prod_{\Psi \in S_n\cdot\Theta} (x - \Psi(\boldsymbol{\alpha})) \in k[x] \quad , \quad \forall \boldsymbol{\alpha} \in V(\mathfrak{S}) \quad . \tag{36}$$

Chacun de ses coefficients est l'évaluation en les racines de f d'un polynôme symétrique en n variable (s'en convaincre). Elle se calcule donc à l'aide de toute forme effective du théorème fondamental des fonctions symétriques. Qu'en est-il du cas général, pour I quelconque ? Nous allons étudier comment calculer $R_{\Theta,I}$ pour un idéal galoisien pur, donc triangulaire.

12.3. La résolvante d'un idéal galoisien pur. Nous fixons I, un idéal galoisien pur de stabilisateur L qui s'identifie à $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$ pour tout $\boldsymbol{\alpha} \in V(I)$.

Pour $\Theta \in k[\boldsymbol{x}]$ et pour tout $\boldsymbol{\alpha} \in V(I)$, la résolvante de notre idéal pur s'exprime ainsi

$$R_{\Theta,I} = \prod_{\Psi \in L\cdot\Theta} (x - \Psi(\boldsymbol{\alpha})) \quad .$$

et elle est indépendante du choix de $\boldsymbol{\alpha} \in \mathrm{V(I)}$.

Considérons $\mathrm{H} := \mathrm{Stab_L}(\Theta) = \{l \in \mathrm{L} \mid l \cdot \Theta = \Theta\}$, un sous-groupe de L ; le polynôme Θ est alors dit être un H-*invariant* L-*primitif*.

Pour $\sigma \in \mathrm{L}$, nous avons :

$$\mathrm{Stab_L}(\sigma \cdot \Theta) = \sigma \mathrm{H} \sigma^{-1} \tag{37}$$

En effet, $\mathrm{Stab_L}(\sigma \cdot \Theta) = \{\tau \in \mathrm{L} \mid \tau \cdot (\sigma \cdot \Theta) = \sigma \cdot \Theta\}$ et $\tau \cdot (\sigma \cdot \Theta) = \sigma \cdot \Theta$ est équivalent à $\sigma^{-1}\tau\sigma \cdot \Theta = \Theta$; d'où $\sigma^{-1}\tau\sigma \in \mathrm{H}$ et $\tau \in \sigma \mathrm{H} \sigma^{-1}$.

REMARQUE 21. Soient $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathrm{V(I)}$. Nous avons $\boldsymbol{\beta} = \boldsymbol{\alpha}^{\sigma}$ avec $\sigma \in \mathrm{L}$ puisque $\mathrm{V(I)} = \mathrm{L} \star \boldsymbol{\alpha}$. Donc $\mathrm{G}_{\boldsymbol{\alpha}} = \mathrm{G}_{\boldsymbol{\beta}^{\sigma^{-1}}} = \sigma \, \mathrm{G}_{\boldsymbol{\beta}} \, \sigma^{-1}$ d'après l'Identité (20). Si, de plus, le groupe de Galois $\mathrm{G}_{\boldsymbol{\beta}} \subset \mathrm{H}$, alors $\mathrm{G}_{\boldsymbol{\alpha}} \subset \sigma \mathrm{H} \sigma^{-1} = \mathrm{Stab_L}(\sigma \cdot \Theta)$.

THÉORÈME 22. *Soient* $\Theta \in k[\boldsymbol{x}]$, $\mathrm{H} := \mathrm{Stab_L}(\Theta)$ *et* $\boldsymbol{\alpha} \in \mathrm{V(I)}$.
(i) S'il existe $\sigma \in \mathrm{L}$ *telle que* $\mathrm{G}_{\boldsymbol{\alpha}} \subset \sigma \mathrm{H} \sigma^{-1}$ *alors la résolvante* $\mathrm{R}_{\Theta,\mathrm{I}}$ *possède une racine dans* k. *Autrement dit, s'il existe* $\boldsymbol{\beta} \in \mathrm{V(I)}$ *tel que* $\mathrm{G}_{\boldsymbol{\beta}} \subset \mathrm{H}$ *alors* $\Theta(\boldsymbol{\beta})$ *est une racine de* $\mathrm{R}_{\Theta,\mathrm{I}}$ *dans* k.
(ii) Inversement, si $\mathrm{R}_{\Theta,\mathrm{I}}$ *possède une racine simple dans* k *alors il existe* $\boldsymbol{\beta} \in \mathrm{V(I)}$ *tel que* $\mathrm{G}_{\boldsymbol{\beta}} \subset \mathrm{H}$ *et donc il existe une permutation* $\sigma \in \mathrm{L}$ *telle que* $\mathrm{G}_{\boldsymbol{\alpha}} \subset \sigma \mathrm{H} \sigma^{-1}$.

DÉMONSTRATION. Montrons la première assertion. Les racines de la résolvante sont les $\tau \cdot \Theta(\boldsymbol{\alpha}) = \Theta(\boldsymbol{\alpha}^{\tau})$ où $\tau \in \mathrm{L}$, un groupe, avec $\mathrm{Stab_L}(\tau \cdot \Theta) = \tau \mathrm{H} \tau^{-1}$. Donc si $\mathrm{G}_{\boldsymbol{\alpha}} \subset \sigma \mathrm{H} \sigma^{-1}$, avec $\sigma \in \mathrm{L}$, alors, en posant $\boldsymbol{\beta} = \boldsymbol{\alpha}^{\sigma}$, il vient : $\mathrm{G}_{\boldsymbol{\beta}} = \sigma^{-1} \mathrm{G}_{\boldsymbol{\alpha}} \sigma \subset \mathrm{H}$ avec $\boldsymbol{\beta} \in \mathrm{V(I)} = \mathrm{L} \star \boldsymbol{\alpha}$. Puisque $\mathrm{H} \cdot \Theta = \Theta$, il en va de même pour G_{β} : $\mathrm{G}_{\boldsymbol{\beta}} \cdot \Theta = \Theta$. Ce qui rend la racine $\theta := \Theta(\boldsymbol{\beta})$ "invariante" par l'action du groupe de Galois $\mathrm{G}_{\boldsymbol{\beta}}$ sur elle. Le théorème de Galois nous dit qu'alors cette racine θ de la résolvante appartient à k.
Inversement, soit $\theta := \Theta(\boldsymbol{\beta})$, avec $\boldsymbol{\beta} \in \mathrm{V(I)}$, une racine de la résolvante appartenant à k. Nous avons alors $g \cdot \Theta(\boldsymbol{\beta}) = \Theta(\boldsymbol{\beta})$ pour tout $g \in \mathrm{G}_{\boldsymbol{\beta}}$ d'après le théorème de Galois. Si de plus cette racine θ est simple, nous avons aussi $g \cdot \Theta = \Theta$ pour tout $g \in \mathrm{G}_{\boldsymbol{\beta}}$. En effet, sinon $(x - \Theta(\boldsymbol{\beta}))(x - g \cdot \Theta(\boldsymbol{\beta}))$ serait un facteur de la résolvante qui produirait une racine au moins double. Puis $\mathrm{G}_{\boldsymbol{\beta}}$ stabilise Θ, il est inclus dans son groupe stabilisateur : $\mathrm{G}_{\boldsymbol{\beta}} \subset \mathrm{H}$. Comme $\boldsymbol{\beta} = \boldsymbol{\alpha}^{\sigma}$ avec $\sigma \in \mathrm{L}$, il vient finalement $\mathrm{G}_{\boldsymbol{\alpha}} = \sigma \, \mathrm{G}_{\boldsymbol{\beta}} \, \sigma^{-1} \subset \sigma \mathrm{H} \sigma^{-1}$. □

EXEMPLE 12.1. Soit $\mathrm{V} = \prod_{1 \le i < j \le n}(x_i - x_j)$ un invariant du groupe alterné A_n dans S_n. Nous avons $\mathrm{S}_n \cdot \mathrm{V} = \{\mathrm{V}, -\mathrm{V}\}$. Posons $v := \mathrm{V}(\boldsymbol{\alpha})$. La résolvante par V relative à l'idéal des relations symétriques est alors :

$$\mathrm{R}_{\mathrm{V},\mathfrak{S}} = x^2 - \Delta(f) = (x - v)(x + v)$$

où $\Delta(f) = \mathrm{Res}_x(f, f') = \prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)^2$ est le discriminant de f (attention : ici le coefficient de x^n dans f est 1 ; sinon il faudrait rajouter un facteur). Si la racine v de

la résolvante n'est pas une racine simple alors $v = -v$ et donc $0 = v^2 = \prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j)^2$, ce qui est impossible car f n'a que des racines simples . Donc notre théorème est toujours applicable à V qui est un invariant dit *universel*. Comme A_n est distingué dans S_n : $\sigma A_n \sigma^{-1} = A_n$ pour tout $\sigma \in S_n$, nous pouvons affirmer le lemme suivant :

LEMME 23. *Le groupe de Galois d'un polynôme f de $k[x]$ est pair (i.e. inclus dans A_n) si et seulement si le discriminant de f est un carré dans k.*

Considérons une transversale à gauche $\{\sigma_1, \ldots, \sigma_n\}$ de L mod H :

$$L = \sigma_1 H + \cdots + \sigma_e H$$

où e est l'indice [L : H] de H dans L. La résolvante est de degré [L : H] car elle s'exprime alors ainsi :

$$R_{\Theta,I} = \prod_{i=1}^{e} (x - \sigma_i.\Theta(\boldsymbol{\alpha})) \quad . \tag{38}$$

où $\boldsymbol{\alpha}$ est un élément quelconque de V(I). Nous voyons que nous avons :

$$\chi_{\Theta,I}(x) = R_{\Theta,I}^{\#H} \quad .$$

Notons que cette expression fournit une nouvelle preuve de l'appartenance de $R_{\Theta,I}$ à $k[x]$ lorsque le corps k est parfait.

Si le H-invariant Θ est de plus $\boldsymbol{\alpha}$-séparable (i.e. $\sigma_i.\Theta(\boldsymbol{\alpha}) \neq \sigma_j\Theta(\boldsymbol{\alpha})$ pour $i \neq j$) alors la résolvante est sans racine multiple et elle s'identifie au polynôme minimal $M_{\Theta,I}$ de l'endomorphisme multiplicatif induit par Θ dans $k[\boldsymbol{x}]/I$.

La résolvante est un polynôme de plus bas degré que le polynôme caractéristique et qui permet de retrouver ce dernier à partir du stabilisateur H de Θ dans le groupe L. Nous voyons bien l'avantage indéniable de la résolvante sur le polynôme caractéristique dans le cadre des idéaux galoisiens.

12.4. Calculer la résolvantes d'un idéal galoisien pur. Nous allons voir comment calculer les résolvantes. Nous reprenons les notations de la section précédente, en supposant encore que I est un idéal galoisien pur.

Nous avons vu comment calculer un polynôme caractéristique. La résolvante peut aisément se déduire de ce calcul qui , sans optimisation, peut s'avérer coûteux.

Nous allons donner une autre méthode pour calculer la résolvante $R_{\Theta,I}$. Elle est basée sur le lemme évident suivant :

LEMME 24. *Soit* G *un sous-ensemble du groupe symétrique* S_n *et* $\Theta \in k[\boldsymbol{x}]$. *Soit* $s(y_1,\dots,y_e) \in k[\boldsymbol{y}]^{S_e}$, *une fonction symétrique de e variables où e est le cardinal de l'orbite* $G\cdot\Theta = \{\Theta_1,\dots,\Theta_e\}$. *Alors le polynôme* $p(\boldsymbol{x}) := s(\Theta_1,\dots,\Theta_e)$ *est invariant par l'action* G *sur* $\boldsymbol{x}$.

D'après ce lemme, si G := Stab(I) et puisque Stab(I) contient $G_{\boldsymbol{\alpha}}$, alors, d'après le Théorème de Galois, $p(\boldsymbol{\alpha}) = s(\Theta_1(\boldsymbol{\alpha}),\dots,\Theta_e(\boldsymbol{\alpha}))$ est invariant par $G_{\boldsymbol{\alpha}}$ donc appartient à k. La valeur $p(\boldsymbol{\alpha})$ dans k est la valeur de classe $[p]$ de p dans $k[\boldsymbol{x}]/I$ obtenue en réduisant p modulo I selon le procédé de divisions euclidiennes successives décrit précédemment.

Nous pouvons donc calculer un à un les coefficients de la résolvante $R_{\Theta,I}$ qui sont à un signe près les fonctions symétriques élémentaires de ses racines $\Theta_1(\boldsymbol{\alpha}),\dots,\Theta_e(\boldsymbol{\alpha})$. L'orbite $L\cdot\Theta$ sera quant à elle calculée par une transversale à gauche de L mod $\mathrm{Stab}_L(\Theta)$ (voir Identité (38) de la résolvante).

Prenons par exemple, le calcul de la constante $a_e \in k$ de la résolvante : on a

$$a_e = (-1)^e p(\boldsymbol{\alpha}) = (-1)^e [p]$$

où $p(\boldsymbol{x}) = \Theta_1 \cdots \Theta_e$. Ici $s(\boldsymbol{y}) = y_1 \cdots y_e$ et la e-ième fonction symétrique élémentaire. On calcule le polynôme $P(\boldsymbol{x}) = [\Theta_1] \cdots [\Theta_e]$ puis sa réduction $[P] = [p]$ modulo I. Puisque les calculs se réalisent dans l'anneau quotient $k[\boldsymbol{x}]/I$, par soucis d'efficacité, on prendra soin de réduire d'abord les polynômes Θ_i de l'orbite avant de calculer les fonctions symétriques élémentaires.

Pour autant, cet algorithme peut s'avérer difficile à mettre en oeuvre car les fonctions symétriques élémentaires sont par leur combinatoire plus coûteuses à calculer directement que les fonctions puissances. Nous privilégions donc l'algorithme qui consiste à calculer d'abord les fonctions puissances des racines de la résolvante pour en déduire les fonctions symétriques élémentaires par les relations de Newton, plus justement appelées de Girard-Newton.

La i-ème fonction puissance des racines de la résolvante est $p_i = [\Theta_1^i + \cdots \Theta_e^i] \in k$. Nous privilégions donc l'algorithme suivant (partiellement parallélisable) : on suppose avoir calculé $p_1,\dots,p_r$ pour $1 \le r < e$ et avoir conservé au passage les $2e$ polynômes réduits $[\Theta_1^j],\dots,[\Theta_e^j]$ pour $j = 1$ et $j = r$. On calcule alors le polynôme

$$P_{r+1} = [\Theta_1][\Theta_1^r] + \cdots + [\Theta_e][\Theta_e^r]$$

puis on en déduit $p_{r+1} = [P_{r+1}] \in k$. Cet algorithme donne d'excellents résultats en pratique.

13. Le théorème de l'élément primitif des idéaux galoisiens

Notre objectif est d'aboutir à l'effectivité du théorème de Galois en partant de celle du théorème fondamental des fonctions symétriques et en passant par celle d'idéaux galoisiens purs intermédiaires. Pour cela, nous allons devoir calculer les générateurs de ces idéaux galoisiens intermédiaires. Nous avons vu que la résolvante est utile à tester si un groupe H contient ou non le groupe de Galois par la présence de racines simples dans k. Nous allons voir, que dans le cas où H contient le groupe de Galois d'un $\boldsymbol{\beta} \in \mathrm{V(I)}$, I galoisien pur, alors des générateurs de $\mathrm{Id}_k(\mathrm{H} \star \boldsymbol{\alpha})$ s'obtiennent à partir de ceux de I et d'un facteur simple dans k d'une résolvante $\mathrm{R}_{\Theta,\mathrm{I}}$, où Θ est tel que $\mathrm{H} = \mathrm{Stab}_{\mathrm{Stab(I)}}(\Theta)$. Ainsi, de proche en proche, il sera possible de calculer un idéal galoisien maximal.

Soient $\mathrm{I} \subset \mathrm{J} \subset \mathfrak{M}_{\boldsymbol{\alpha}}$ des idéaux galoisiens du polynôme séparable $f = \prod_{i=1}^{n}(x - \alpha_i) \in k[x]$ avec $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n)$.

DÉFINITION 13.1. Un polynôme $p \in k[\boldsymbol{x}]$ est dit I-*primitif de l'idéal* J si

$$\mathrm{Inj}(\mathrm{J}, \mathfrak{M}_{\boldsymbol{\alpha}}) = \{\sigma \in \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}}) \mid \sigma \cdot p(\boldsymbol{\alpha}) = 0\} \quad .$$

LEMME 25. *Soient* I *un idéal galoisien,* $\mathrm{L} := \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}}) = \mathrm{G}_{\boldsymbol{\alpha}}\mathrm{L}$ *et* H *un sous-groupe de* S_n. *Supposons que* $\mathrm{J} = \mathrm{Id}(\mathrm{H} \star \boldsymbol{\alpha})$. *Soit* $\Theta \in k[\boldsymbol{x}]$ *tel que* $\mathrm{Stab}_{\mathrm{L}}(\Theta) = \mathrm{H}$. *Supposons que* $\theta := \Theta(\boldsymbol{\alpha})$ *soit une racine simple de la résolvante* $\mathrm{R}_{\Theta,\mathrm{I}}$. *Alors* $p(\boldsymbol{x}) = \min_{\theta,k}(\Theta)$ *est un polynôme* I-*primitif de l'idéal* J.

DÉMONSTRATION. Nous avons $p \in k[\boldsymbol{x}]$ et $p(\boldsymbol{\alpha}^h) = p(\boldsymbol{\alpha}) = \min_{\theta,k}(\theta) = 0$ pour tout $h \in \mathrm{H}$ puisque H stabilise Θ. Donc $p \in \mathrm{J}$. L'inclusion $\mathrm{Inj}(\mathrm{J}, \mathfrak{M}_{\boldsymbol{\alpha}}) \subset \mathrm{L}$ étant déjà établie par la correspondance galoisienne, l'inclusion "$\subset$" de la Définition 13.1 est satisfaite. Montrons que p est bien primitif avec l'inclusion inverse. Soit une permutation $\sigma \in \mathrm{L}$ telle $\sigma \cdot p(\boldsymbol{\alpha}) = 0$; c'est à dire $\sigma \cdot \Theta(\boldsymbol{\alpha})$ est une racine de $\min_{\theta,k}$. D'après le Théorème 6, les racines de $\min_{\theta,k}$ sont les $g \cdot \Theta(\boldsymbol{\alpha})$ où g parcourt $\mathrm{G}_{\boldsymbol{\alpha}}$. Donc, il existe une permutation $g \in \mathrm{G}_{\boldsymbol{\alpha}}$ telle que $\sigma \cdot \Theta(\boldsymbol{\alpha}) = g \cdot \Theta(\boldsymbol{\alpha})$. Comme $g^{-1} \in \mathrm{G}_{\boldsymbol{\alpha}}$, l'action de $\mathrm{G}_{\boldsymbol{\alpha}}$ sur $k(\boldsymbol{\alpha})$ nous autorise permuter par g^{-1} de part et d'autre de cette égalité. D'où $g^{-1}\sigma \cdot \Theta(\boldsymbol{\alpha}) = \Theta(\boldsymbol{\alpha}) = \theta$. Comme θ est une racine simple de la résolvante et $g^{-1}\sigma \in \mathrm{G}_{\boldsymbol{\alpha}}\mathrm{L} = \mathrm{L}$, nous en déduisons que $\Theta = (g^{-1}\sigma) \cdot \Theta$. D'où $g^{-1}\sigma \in \mathrm{H} = \mathrm{Stab}_{\mathrm{L}}(\Theta)$. Et enfin, puisqu'alors $\sigma \in \mathrm{G}_{\boldsymbol{\alpha}}\mathrm{H} = \mathrm{Inj}(\mathrm{J}, \mathfrak{M}_{\boldsymbol{\alpha}})$, le polynôme p est bien I-primitif de l'idéal J. □

Notons que $\min_{\theta,k}$ est un facteur de la résolvante $\mathrm{R}_{\Theta,\mathrm{I}}$ et que ce facteur est simple si et seulement si θ est une racine simple de la résolvante.

EXEMPLE 13.1. Soit $\Theta = t_1 x_1 + \cdots + t_n x_n$ (ou bien $\Theta = x_1^{t_1} \cdots x_n^{t_n}$) où les t_i sont des entiers deux-à-deux distincts. Comme $\mathbb{Q}$ est infini, on peut choisir les coefficients t_i tels que θ soit une racine simple de la résolvante $\mathrm{R}_{\Theta,\mathrm{I}}$ (en fait, c'est le cas en dehors d'un nombre

fini de valeurs t_i). Alors $\min_{\theta,\mathbb{Q}}(\Theta)$ est un polynôme I-primitif de l'idéal $\mathfrak{M}_{\boldsymbol{\alpha}}$. En effet, ici $H = I_n$ donc $J = Id(\boldsymbol{\alpha}) = \mathfrak{M}_{\boldsymbol{\alpha}}$. On a bien $Inj(J, \mathfrak{M}_{\boldsymbol{\alpha}}) = G_{\boldsymbol{\alpha}} I_n = G_{\boldsymbol{\alpha}}$. Le polynôme $R_{\Theta,\mathfrak{S}}$ est la *résolvante de Galois* sur laquelle Evariste Galois s'appuya pour bâtir sa fameuse théorie.

EXEMPLE 13.2. Pour $H = A_n$, nous pouvons choisir l'invariant universel, le Vandermond V vu précédemment. Si le discriminant de f est un carré v^2 dans k, i.e. avec $v \in k$, alors $x - v$ est le polynôme minimal de v sur $\mathbb{Q}$ et $V - v$ est un polynôme S_n-primitif de l'idéal $Id_k(A_n \star \boldsymbol{\alpha})$. Nous avions déjà vu dans un exemple précédent que $G_{\boldsymbol{\alpha}} \subset A_n$.

Exercice de réflexion : Que peut-on dire lorsque $H = G_{\boldsymbol{\alpha}}$?

THÉORÈME 26. *(Elément primitif). Soient* $I \subset J$ *deux idéaux galoisiens de* $f \in k[x]$. *Si* $p \in k[\boldsymbol{x}]$ *est un polynôme* I*-primitif de l'idéal* J *alors*

$$J = I + < p >$$

Ce théorème fondamental sera démontré plus loin. Nous pouvons le commenter. Supposons que l'idéal galoisien I soit pur et que la résolvante $R_{\Theta,I}$ possède une racine simple λ dans k. Alors nous savons qu'il existe $\boldsymbol{\beta} \in V(I)$ tel que $G_{\boldsymbol{\beta}} \subset H = Stab_L(\Theta)$ et $\lambda = \Theta(\boldsymbol{\beta})$ (n'oublions pas que $R_{\Theta,I}$ ne dépend pas du choix de $\boldsymbol{\alpha}$ dans $V(I)$). Donc $J = Id(H \star \boldsymbol{\beta})$ est un idéal galoisien pur de groupe de décomposition H. Ce que nous ne pouvons pas faire en numérique, nous le pouvons en algèbre. En effet, en algèbre, nous pouvons choisir $\boldsymbol{\beta} \in V(I)$; cela est différent en numérique où les calculs sont réalisés avec une approximation des racines dont l'ordre est figé. Le polynôme $\Theta - \lambda$ est un polynôme I-primitif de l'idéal $J = Id(H \star \boldsymbol{\alpha})$. Donc nous obtenons l'idéal galoisien pur J avec le théorème de l'élément primitif :

$$J = I + < \Theta - \lambda > \quad .$$

Nous voyons que de proche en proche nous construirons une chaîne strictement croissante d'idéaux galoisiens purs (donc triangulaires) $J_1, \ldots, J_s$ telle que

$$J_1 = \mathfrak{S} \subsetneq J_2 \subsetneq \cdots \subsetneq J_s = \mathfrak{M}$$

qui s'arrêtera à l'idéal maximal $J_s = \mathfrak{M}$ quand, pour tout sous-groupe H de $Stab(J_s)$ contenant le "groupe de Galois", et pour Θ un H-invariant $Stab(J_s)$-primitif, la résolvante R_{Θ,J_s} n'aura pas de facteur dans k (il faudra éventuellement changer d'invariant lorsqu'une racine multiple appartiendra à k).

PREUVE DU THÉORÈME DE L'ÉLÉMENT PRIMITIF. Posons $\mathfrak{M} := \mathfrak{M}_{\boldsymbol{\alpha}}$, $L := Inj(I, \mathfrak{M})$ et $G := G_{\boldsymbol{\alpha}}$. Nous avons $U := Inj(J, \mathfrak{M}) \subset L$. Notons $U' \subset S_n$ tel que $L = U + U'$ et posons $J' := Id(U' \star \boldsymbol{\alpha})$. Nous avons alors $I = J \cap J'$. Pour les injecteurs, nous avons $U = GU$ et $L = GL$ puisque ce sont les injecteurs d'idéaux galoisiens dans $\mathfrak{M}$. Donc $U + U' = L = GL = GU + GU' = U + GU'$. D'où $U' = GU' = Inj(J', \mathfrak{M})$. Comme les racines α_i sont deux-à-deux distinctes et les ensembles de permutations U et U′ sont disjoints, les variétés

$V(J) = U \star \boldsymbol{\alpha}$ et $V(J') = U' \star \boldsymbol{\alpha}$ aussi sont disjointes : elles vérifient $V(J) \cap V(J') = \emptyset$. Ainsi J et J' sont comaximaux. D'où $1 \in J + J'$ et il existe $u \in J$ et $v \in J'$ tels que $1 = u + v$.
Par ailleurs, comme $V(J + p) \subset V(\mathfrak{S}) = S_n \star \boldsymbol{\alpha}$,

$$V(I + p) = \{\boldsymbol{\alpha}^\sigma \mid \sigma \in \mathrm{Inj}(I, \mathfrak{M}) \text{ et } p(\boldsymbol{\alpha}^\sigma) = 0\} = \{\boldsymbol{\alpha}^\sigma \mid \sigma \in \mathrm{Inj}(J, \mathfrak{M})\} \quad ,$$

par définition des éléments I-primitifs de l'idéal J. D'où $V(I + p) = V(J)$ et donc l'idéal J est le radical de $I + p$. Nous voulons montrer l'égalité entre ces deux idéaux. Puisque les variétés sont identiques, il existe un entier $m > 0$ tel que

$$J^m \subset I + p \subset J$$

où $J^m = \{r_1 \cdots r_m \mid r_i \in J\}$. Soit $r \in J$. Puisque $1 = u + v$, nous avons $r = ru + rv$ avec $u \in J$ et $v \in J'$. D'une part, $ru \in J^m \subset I + p$. Et, d'autre part, $rv \in JJ' = J \cap J'$ puisque J et J' sont comaximaux. Puisque $J \cap J' = I \subset I + p$, nous avons aussi $rv \in I + p$. D'où $r = ru + rv \subset I + p$ et donc $J \subset I + p \subset J$. L'égalité est bien prouvée et la démonstration s'achève. □

La démonstration de théorème de l'élément primitif repose en parti sur ce lemme (démontré également dans le cours 9) :

LEMME 27. *Soient* $J, I_1, \ldots, I_s$ *des idéaux 2-à-2 comaximaux. Alors* J *et* $\bigcap I_j$ *sont comaximaux. Par conséquent, si* $J_1, \ldots, J_r, I_1, \ldots, I_s$ *sont des idéaux 2-à-2 comaximaux alors les idéaux* $\bigcap J_j$ *et* $\bigcap I_j$ *sont aussi comaximaux.*

DÉMONSTRATION. Comme nos idéaux sont galoisiens, toutes les variétés son finies et tout idéal maximal est aussi premier. D'abord remarquons que si une intersection d'idéaux est incluse dans un idéal premier $\mathfrak{M}$ alors l'un d'eux est inclus dans $\mathfrak{M}$. En effet, sinon pour chaque idéal de l'intersection, on trouverait un élément p_i qui n'appartient pas à $\mathfrak{M}$ alors que pourtant le produit des p_i lui appartient. Ce qui est impossible puisque $\mathfrak{M}$ est premier.
Supposons que J et $\bigcap I_j$ ne soient pas comaximaux. Il existe alors un idéal maximal $\mathfrak{M}$ qui les contient à la fois. Donc $\mathfrak{M}$ qui est aussi premier contient J et l'un au moins des idéaux I_j ; ce qui est impossible par hypothèse. □

14. Complément : Décomposition d'un idéal galoisien et de sa variété

Nous fixons un idéal galoisien $I := I^L_{\boldsymbol{\alpha}}$.

Considérons l'union disjointe de classes à droite

$$\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}}) = G_{\boldsymbol{\alpha}} L = G_{\boldsymbol{\alpha}} \tau_1 + \cdots + G_{\boldsymbol{\alpha}} \tau_s \quad .$$

L'ensemble $\{\tau_1, \ldots, \tau_s\}$ est appelé une *transversale à droite* de L $\mod G_{\boldsymbol{\alpha}}$.

La variété $V(I) = G_{\boldsymbol{\alpha}} L \star \boldsymbol{\alpha}$ est par conséquent l'union disjointe des s variétés irréductibles $V(\tau_i^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}}) = G_{\boldsymbol{\alpha}} \tau_i \star \boldsymbol{\alpha}$ (voir Identité (21)) ; chacune est irréductible car variété d'un idéal maximal $\tau_i^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}} = \mathfrak{M}_{\boldsymbol{\alpha}^{\tau_i}}$ (voir dentité (19)), donc premier puisque sa variété est finie.

Posons $\mathfrak{M}_i = \mathfrak{M}_{\boldsymbol{\alpha}^{\tau_i}}$ pour $i \in [\![1, s]\!]$. La variété de I se décompose en s irréductibles distinctes (et donc disjointes) :

$$V(I) = V(\mathfrak{M}_1) \cup \cdots \cup V(\mathfrak{M}_1)$$

Donc l'idéal galoisien défini par $(L, \boldsymbol{\alpha})$ est l'intersection suivante d'idéaux maximaux deux-à-deux distincts (ils sont donc co-maximaux) :

$$I_{\boldsymbol{\alpha}}^L = \bigcap_{i=1}^{s} \mathfrak{M}_i = \prod_{i=1}^{s} \mathfrak{M}_i$$

puisque pour deux idéaux I, J co-maximaux $I \cap J = IJ$. Posons $\mathfrak{M} := \mathfrak{M}_{\boldsymbol{\alpha}}$. Nous en déduisons que

$$k[\boldsymbol{x}]/I = k[\boldsymbol{x}]/\prod_{i=1}^{s} \mathfrak{M}_i = \prod_{i=1}^{s} k[\boldsymbol{x}]/\mathfrak{M}_i \simeq k(\boldsymbol{\alpha})^s$$

d'après le théorème chinois des restes puisque les idéaux $\mathfrak{M}_1, \ldots, \mathfrak{M}_s$ sont deux-à-deux premiers entre eux (en fait, premiers et deux-à-deux distincts).

Lorsque $L = S_n$, s est l'indice du groupe de Galois $G_{\boldsymbol{\alpha}}$ dans S_n qui est donc l'intersection de s idéaux maximaux deux-à-deux distincts que l'on obtient rapidement par le calcul à partir d'un seul d'entre eux car le groupe de décomposition d'un idéal galoisien se calcule facilement et rapidement (Exercice).

Pour un exemple, vous êtes invités à consulter l'exercice 5 avec son corrigé dans l'examen de Mai 2017 disponible sur https ://webusers.imj-prg.fr/~pierre.charollois/calcul-alg2017.html

15. Un exemple complet : Examen 2017

Nous donnons ici une correction détaillée d'un exercice de l'examen 2017. À des fins pédagogiques, certaines réponses sont plus longues et détaillées que ce qui était demandé.

Nous considérons le polynôme $f := x^6 + 2$ irréductible sur $\mathbb{Q}$ et un 6-uplet $\boldsymbol{\alpha}$ composé des racines de f. Soit le sous-groupe $L := PGL(2,5)$ du groupe symétrique S_6 d'ordre 120. L'idéal galoisien $I := I_{\boldsymbol{\alpha}}^L$ de $\mathbb{Q}[x_1,\ldots,x_6]$ est engendré par l'ensemble triangulaire $\{f_1,\ldots,f_6\}$ suivant :

$$
\begin{aligned}
I \;=\; < \quad & f_1 := x_1^6 + 2\,, \\
& f_2 := x_2^5 + x_2^4 x_1 + x_2^3 x_1^2 + x_2^2 x_1^3 + x_2 x_1^4 + x_1^5\,, \\
& f_3 := x_3^4 + x_3^3 x_2 + x_3^3 x_1 + x_3^2 x_2^2 + x_3^2 x_2 x_1 + x_3^2 x_1^2 + x_3 x_2^3 + x_3 x_2^2 x_1 + x_3 x_2 x_1^2 \\
& \qquad + x_3 x_1^3 + x_2^4 + x_2^3 x_1 + x_2^2 x_1^2 + x_2 x_1^3 + x_1^4\,, \\
& f_4 := 24 x_4 + 5 x_3^3 x_2^4 + 6 x_3^3 x_2^3 x_1 + 8 x_3^3 x_2^2 x_1^2 + x_3^3 x_2 x_1^3 + 8 x_3^2 x_2^4 x_1 + 4 x_3^2 x_2^3 x_1^2 + 8 x_3^2 x_2^2 x_1^3 \\
& \qquad + 12 x_3 x_2^4 x_1^2 + 10 x_3 x_2^3 x_1^3 + 4 x_3 x_2^2 x_1^4 + 4 x_3 x_2 x_1^5 + 4 x_3 + 5 x_2^4 x_1^3 + 14 x_2 + 12 x_1\,, \\
& f_5 := 24 x_5 - 5 x_3^3 x_2^4 - 7 x_3^3 x_2^3 x_1 - 16 x_3^3 x_2^2 x_1^2 - 7 x_3^3 x_2 x_1^3 - 5 x_3^3 x_1^4 - 8 x_3^2 x_2^4 x_1 - 12 x_3^2 x_2^3 x_1^2 \\
& \qquad - 12 x_3^2 x_2^2 x_1^3 - 8 x_3^2 x_2 x_1^4 - 12 x_3 x_2^4 x_1^2 - 16 x_3 x_2^3 x_1^3 - 12 x_3 x_2^2 x_1^4 + 8 x_3 - 5 x_2^4 x_1^3 \\
& \qquad - 5 x_2^3 x_1^4 - 2 x_2 - 2 x_1\,, \\
& f_6 := x_6 + x_5 + x_4 + x_3 + x_2 + x_1 > \;.
\end{aligned}
$$

Soit $\Theta := x_1x_4 + x_4x_5 + x_5x_2 + x_2x_3 + x_3x_6 + x_6x_1$ de stabilisateur H dans L.
La résolvante de Θ par I vaut $R_{\Theta,I} = x(x^3-2)(x^3+2)^2$.

(1) Pourquoi l'idéal I est-il pur et stabilisateur le groupe L ?
Réponse : D'après le cours, comme L définit I avec $\boldsymbol{\alpha}$, L est inclus dans l'injecteur M de I dans $I_{\boldsymbol{\alpha}}$ (on a toujours $M = G_\alpha L$). Le cardinal de cet injecteur M est 120, le produit des degrés initiaux de l'ensemble triangulaire engendrant I (cours), identique à l'ordre du groupe L. Donc M = L. Comme l'injecteur de I dans $I_{\boldsymbol{\alpha}}$ est un groupe, il s'identifie au stabilisateur de I qui par conséquent est galoisien pur. *Rappelons qu'un idéal galoisien pur est triangulaire mais que tout idéal galoisien triangulaire n'est pas nécessairement pur.*

(2) Pourquoi le groupe H est-il d'ordre 12 ?
Réponse : Le degré 10 de la résolvante est identique à l'indice [L : H] de H dans L, d'ordre 120. Formule de Lagrange : $120 = \#L = [L:H]\,\#H = 10\#H$.

(3) Soit $G_{\boldsymbol{\alpha}}$ le groupe de décomposition de $Id(\boldsymbol{\alpha})$, un des idéaux maximaux contenant I. Pourquoi peut-on choisir $\boldsymbol{\alpha} \in V(I)$ tel que $G_{\boldsymbol{\alpha}} \subset H$? Fixons ce $\boldsymbol{\alpha}$.

Réponse : Car $R_{\Theta,I}$, une résolvante L-relative par un H-invariante L-relatif, possède une racine **simple** dans $\mathbb{Q}$ (cours).

(4) Pourquoi $I_{\boldsymbol{\alpha}}^H$ est-il un idéal galoisien pur ? (expliquez en deux mots)
Réponse : Car $G_\alpha \subset H$. Donc H est à la fois le groupe de décomposition de I et son injecteur dans $I_{\boldsymbol{\alpha}}$ (cours).

(5) Donnez un système de générateurs non nécessairement triangulaire de l'idéal $I_{\boldsymbol{\alpha}}^H$ à partir de I, un facteur de $R_{\Theta,I}$ et Θ.
Réponse : Prenons le facteur simple x et remplaçons x par l'invariant Θ : $I_{\boldsymbol{\alpha}}^H = I + <\Theta>$, d'après le théorème de l'élément primitif du cours.

(6) Soit J l'idéal engendré par l'ensemble triangulaire suivant :

$$J = < g_1 := x_1^6 + 2\,,\quad g_2 := x_2 + x_1\,,\quad g_3 := x_3^2 + x_1x_3 + x_1^2\,,$$
$$g_4 := x_4 + x_3\,,\quad g_5 := x_5 + x_3 + x_1\,,\quad g_6 := x_6 - x_3 - x_1 > .$$

En utilisant la dérivée de g_3 en x_3, montrez que la variété V(J) est de cardinal 12.
Réponse : (à des fins pédagogiques, elle est bien plus longue que ce qui était demandé). Ici, J étant engendré par un ensemble triangulaire, l'ensemble de ses solutions comptées avec leurs multiplicités, est le produit 12 des degrés initiaux de l'ensemble triangulaire l'engendrant et de la forme $(\alpha_1,\ldots,\alpha_6)$ où $\alpha_1,\ldots,\alpha_6$ sont les 6 racines distinctes de x^6+2, irréductible sur $\mathbb{Q}$ donc séparable (cours). Il suffit de prouver que les solutions de J sont deux-à-deux distinctes. Soit α_1, une racine de $g_1(x)$; d'après l'ensemble triangulaire engendrant J, les solutions de J telles que $g_1(\alpha_1) = 0$ sont les 6-uplets $\boldsymbol{\alpha} := (\alpha_1, \alpha_2 := -\alpha_1, \alpha_3, \alpha_4 := -\alpha_3, \alpha_5 := -\alpha_3 - \alpha_1, \alpha_6 := \alpha_3 + \alpha_1)$ et $\boldsymbol{\alpha}' := (\alpha_1, -\alpha_1, \beta_3, -\beta_3, -\beta_3 - \alpha_1, \beta_3 + \alpha_1)$ de $V(I_{\boldsymbol{\alpha}}^{S_n})$ où $G_3 := g_3(\alpha_1, -\alpha_1, x) = x^2 + \alpha_1 x + \alpha_1^2 = (x-\alpha_3)(x-\beta_3)$. Montrons que G_3 possède deux racines distinctes. Si la dérivée $G_3' = 2x + \alpha_1$ s'annule en $\alpha_3 = \beta_3$ alors $\alpha_1 = -2\alpha_3$. Dans ce cas, $\alpha_6 = \alpha_3 + \alpha_1 = \alpha_3 - 2\alpha_3 = \alpha_4$. Ce qui est impossible puisque les racines de x^6+2 sont deux-à-deux distinctes. Donc $\boldsymbol{\alpha}$ et $\boldsymbol{\alpha}'$ sont deux solutions distinctes de J. Comme g_1 possède 6 racines distinctes, le cardinal de V(J) est bien $12 = 2\cdot 6$. L'idéal J est triangulaire donc radical.

Note : En considérant $\boldsymbol{\alpha}$, nous remarquons que $\alpha_1,\ldots\alpha_6$ sont bien les racines distinctes de x^6+2 ; puisque $\alpha_3^2+\alpha_1\alpha_3+\alpha_1^2 = 0$, nous avons $x^2+\alpha_1 x+\alpha_1^2 = (x-\alpha_3)(x-\alpha_5)$ et $x^2-\alpha_1 x+\alpha_1^2 = (x-\alpha_4)(x-\alpha_6)$; d'où $(x-\alpha_1)\cdots(x-\alpha_6) = (x-\alpha_1)(x+\alpha_1)(x^2+\alpha_1 x+\alpha_1^2)(x^2-\alpha_1 x+\alpha_1^2) = x^6-\alpha_1^6 = x^6+2$.

Remarque : *Rappelons que pour* I *un idéal de* $R = Q[x_1,\ldots,x_6]$, $\#V(I) = \dim_{\mathbb{Q}} R/\sqrt{I}$ *est inférieur à* $\dim_{\mathbb{Q}} R/I$ *et que* I *est radical si et seulement si il y a égalité.*

(7) On admet que I est inclus dans J.
Dites comment vous vérifieriez cette affirmation. Illustrez la méthode en effectuant

parmi les calculs nécessaires uniquement celui qui concerne le polynôme f_6.
Réponse : Il suffit de réduire chaque f_i modulo J au moyen de 6 divisions euclidiennes ; $r_6 := f_i$ et $r_j = q_j g_i + r_{i-1}$. On a $r_0 = 0$ si et seulement si $f_i \in J$. On voit que, modulo J, $[f_6] = [x_6 + x_5 + x_4 + x_3 + x_2 + x_1 = (x_3 + x_1) + x_5 + x_4 + x_3 + x_2 + x_1] = [(x_3 + x_1) - (x_3 + x_1) + x_4 + x_3 + x_2 + x_1] = [-x_3 + x_3 + x_2 + x_1] = [-x_1 + x_1] = [0]$.

(8) Montrez que $I_{\boldsymbol{\alpha}}^{H} = J$.
Réponse : D'après la question 6, l'idéal J est radical et sa variété est de cardinal 12. Le cardinal de la variété de l'idéal galoisien **pur** $I_{\boldsymbol{\alpha}}^{H}$ est aussi 12, le cardinal de H, son groupe de décomposition. Puisque $I_{\boldsymbol{\alpha}}^{H} = I + < \Theta >$ et $I \subset J$, pour que ces ceux idéaux radicaux soient identiques (i.e. que leurs variétés soient identiques), il faut et il suffit que $\Theta \in J$. En remplaçant x_2 par $-x_1$, x_4 par $-x_3$, x_5 par $-(x_1 + x_3)$ et x_6 par $x_1 + x_3$, modulo J, nous avons : $[\Theta] := [x_1x_4 + x_4x_5 + x_5x_2 + x_2x_3 + x_3x_6 + x_6x_1] = [-x_1x_3 + x_3(x_1 + x_3) + (x_1 + x_3)x_1 - x_1x_3 + x_3(x_1 + x_3) + (x_1 + x_3)x_1] = [2x_1^2 + 2x_3^2 + 2x_1x_3] = [2g_3] = [0]$. Donc Θ se réduit bien à 0 modulo J et $J = I_{\boldsymbol{\alpha}}^{H}$.

(9) Le groupe H admet pour générateurs les permutations

$$\sigma_1 := (1,2)(3,4)(5,6),\ \sigma_2 := (1,3,5)(2,4,6),\ \sigma_3 := (3,5)(4,6) \quad .$$

Comment pourriez-vous vérifier que H est bien le stabilisateur de J ? Illustrez la méthode en traitant uniquement deux polynômes de votre choix.
Réponse : Il suffit de vérifier que pour chaque générateur g_i de J et chaque permutation σ engendrant H, on a $\sigma \cdot g_i \in J$. Nécessairement, pour $j = 1,2,3$, $\sigma_j \cdot g_1(x_1) = g_1(x_l) \in J$ puisque $g_1(\alpha_l) = 0$ pour tout $l \in [1,6]$. Aussi $\sigma_1 \cdot g_2 = \sigma_3 \cdot g_2 = g_2 \in J$ et $\sigma_2 \cdot g_2 = x_3 + x_4 = g_4 \in J$.

(10) Le seul sous-groupe transitif de H est C_6 d'ordre 6. Nous supposons avoir trouvé $\Psi \in \mathbb{Q}[x_1, \ldots, x_6]$ de stabilisateur C_6 dans H, dont la résolvante $R_{\Psi,J}$ est sans racine dans $\mathbb{Q}$. Qu'en concluez-vous ?
Réponse : Comme $x^6 + 2$ est irréductible sur $\mathbb{Q}$, le groupe de Galois $G_{\boldsymbol{\alpha}}$ de $\boldsymbol{\alpha}$ sur $\mathbb{Q}$ est un sous-groupe transitif de S_6 (cours). Donc $G_\alpha = H$ ou $G_\alpha = C_6$ puisque $G_\alpha \subset H$. La H-résolvante C_6-relative $R_{\Psi,J}$ ne possédant aucune racine dans $\mathbb{Q}$, $G_{\boldsymbol{\alpha}}$ n'est inclus dans aucun conjugué de C_6 dans H (cours). Nous en concluons que $G_{\boldsymbol{\alpha}} = H$ et J est l'idéal (maximal) des relations $\mathrm{Id}(\boldsymbol{\alpha})$.

(11) Soit le polynôme $\Gamma := x_1x_3x_5 + x_2x_4x_6$. Expliquez pourquoi $\Gamma(\boldsymbol{\alpha})$ appartient à $\mathbb{Q}$. Quelle procédure proposez-vous pour calculer la valeur de $\Gamma(\boldsymbol{\alpha})$?
Calculez $\Gamma(\boldsymbol{\alpha})$.
Réponse : Avec les 3 générateurs de H, on vérifie facilement que Γ est invariant par H. Comme H est le groupe de Galois de $\boldsymbol{\alpha}$ sur $\mathbb{Q}$, par le théorème de Galois, $\Gamma(\boldsymbol{\alpha})$ appartient à $\mathbb{Q}$ (cours). Nous avons $\Gamma - \Gamma(\boldsymbol{\alpha}) \in J$. Pour obtenir la valeur $\Gamma(\boldsymbol{\alpha})$, il suffit de réduire Γ modulo J : comme, d'après les générateurs g_2, g_4, g_5 et g_6 de J, nous avons $\alpha_1 = -\alpha_2$, $\alpha_4 = -\alpha_3$ et $\alpha_6 = -\alpha_5$, nous obtenons $\Gamma(\boldsymbol{\alpha}) := \alpha_1\alpha_3\alpha_5 - \alpha_1\alpha_3\alpha_5 = 0$.

16. Vademecum - Annick Valibouze - Sorbonne Université

Nous fixons le corps $k := \mathbb{Q}$ (ou tout corps parfait) et un polynôme f (unitaire) d'une variable x :

$$f(x) := (x-\alpha_1)\cdots(x-\alpha_n) \in k[x]$$

à coefficients dans k.Les racines $\alpha_1,\ldots,\alpha_n$ de f sont supposées deux-à-deux distinctes. Le polynôme f est alors dit *séparable* ou sans facteur carré ou encore sans facteur multiple. Fixons un n-uplet $\boldsymbol{\alpha} := (\alpha_1,\ldots,\alpha_n)$ de ses racines.

$$(\boldsymbol{\alpha}^\tau)^\sigma \quad = \quad \boldsymbol{\alpha}^{\tau\sigma} \qquad (2)$$

$$\sigma\cdot p(\boldsymbol{\alpha}^\tau) \quad = \quad p(\boldsymbol{\alpha}^{\tau\sigma}) = \tau\sigma\cdot p(\boldsymbol{\alpha}) \qquad (3) \qquad .$$

INJECTEURS ET STABILISATEURS

$$\mathrm{Inj}(I,J) := \{\sigma\in S_n \mid \sigma\cdot I\subset J\} \qquad \mathrm{Stab}(I) := \mathrm{Inj}(I,I) \quad .$$

Nous avons tout naturellement $\mathrm{Inj}(I,J)\cdot I\subset J$.

$$S_n = \mathrm{Stab}(\mathfrak{S}) = \mathrm{Inj}(\mathfrak{S},\mathfrak{M}_{\boldsymbol{\alpha}})$$

$$\mathrm{Gal}_k(\boldsymbol{\alpha}) = \mathrm{Stab}(\mathfrak{M}_{\boldsymbol{\alpha}}) = \mathrm{Inj}(\mathfrak{M}_{\boldsymbol{\alpha}},\mathfrak{M}_{\boldsymbol{\alpha}})$$

$$\text{Si} \quad I\subseteq J \quad \text{alors} \quad \mathrm{Stab}(I)\subseteq \mathrm{Inj}(I,J) \qquad (23)$$

$$\text{Si} \quad I\subseteq \mathfrak{M}_{\boldsymbol{\alpha}} \quad \text{alors} \quad \mathrm{Gal}_k(\boldsymbol{\alpha})\subset \mathrm{Inj}(I,\mathfrak{M}_{\boldsymbol{\alpha}}) \quad (25)$$

$$\mathrm{Inj}(\sigma\cdot I,\tau\cdot J) = \tau\,\mathrm{Inj}(I,J)\,\sigma^{-1} \quad (26)$$

IDEAL MAXIMAL DES RELATIONS ET CORPS DES RACINES

Théorème de Galois 4. *Soit* $\gamma \in k(\boldsymbol{\alpha})$. *Pour que* $\gamma \in k$ *il faut et il suffit que que* $\gamma^{\sigma} = \gamma$ *pour tout* $\sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})$.

Théorème de Galois 6. *Soit* $\theta \in k(\boldsymbol{\alpha})$. *Alors* $\min_{\theta,k}$, *son polynôme minimal sur k, est celui dont les racines sont les éléments de l'orbite de* θ *sous l'action du groupe de Galois de* $\boldsymbol{\alpha}$ *sur k :*

$$\min_{\theta,k} = \prod_{\gamma \in \mathrm{Gal}_k(\boldsymbol{\alpha}) \star \theta} (x - \gamma) = \mathrm{M}_{\hat{\Theta},\mathfrak{M}_{\boldsymbol{\alpha}}} \quad .$$

Isomorphisme entre l'anneau quotient $\mathrm{A} := k[\boldsymbol{x}]/\mathfrak{M}_{\boldsymbol{\alpha}}$ et le corps $k(\boldsymbol{\alpha})$:

$$k[\boldsymbol{x}]/\mathfrak{M}_{\boldsymbol{\alpha}} \simeq k(\boldsymbol{\alpha}) \quad .$$

Variété idéal des $\boldsymbol{\alpha}$-relation :

$$\mathrm{V}(\mathfrak{M}_{\boldsymbol{\alpha}}) = \mathrm{Gal}_k(\boldsymbol{\alpha}) \star \boldsymbol{\alpha} \qquad (13)$$

$$\mathfrak{M}_{\boldsymbol{\alpha}} = \mathrm{Id}_k(\boldsymbol{\alpha}) = \mathrm{Id}_k(\mathrm{H} \star \boldsymbol{\alpha}) = \mathrm{Id}_k(\mathrm{Gal}_k(\boldsymbol{\alpha}) \star \boldsymbol{\alpha}) \qquad \forall \mathrm{H} \subset \mathrm{Gal}_k(\boldsymbol{\alpha})$$

$$\dim_k k(\boldsymbol{\alpha}) = \mathrm{Card}(\mathrm{V}(\mathfrak{M}_{\boldsymbol{\alpha}})) = \mathrm{Card}(\mathrm{Gal}_k(\boldsymbol{\alpha})) \quad .$$

Soit $\theta \in k(\boldsymbol{\alpha})$ et un polynôme $\Theta \in k[\boldsymbol{x}]$ tel que $\theta := \Theta(\boldsymbol{\alpha})$. Pour tout $\sigma \in \mathrm{G}_{\boldsymbol{\alpha}}$, nous pouvons adopter cette notation pour l'action de σ sur θ :

$$\theta^{\sigma} := \sigma \cdot \Theta(\boldsymbol{\alpha}) = \Theta(\boldsymbol{\alpha}^{\sigma}) \quad .$$

L'idéal des $\boldsymbol{\alpha}$-relations $\mathfrak{M}_{\boldsymbol{\alpha}}$ est triangulaire : il est engendré par un ensemble triangulaire séparable réduit formé par les *modules fondamentaux* de Tchebotarev :

$$\mathfrak{F}_1(x_1, \ldots x_n), \ldots, \mathfrak{F}_n(x_n) \quad \text{avec } \mathfrak{F}_i \in k[x_i, \ldots, x_n]$$

Posons $k_{n+1} := k$ et $k_i := k_{i+1}(\alpha_i) = k(\alpha_{i+1}, \ldots, \alpha_n)$. Pour tout $i \in [\![1, n]\!]$, $\mathfrak{F}_i(x_i, \alpha_{i+1}, \ldots, \alpha_n) = \min_{\alpha_i, k_{i+1}}(x_i)$. On a ainsi $k_i \simeq k[x_i, \ldots, x_n]/ < \mathfrak{F}_i, \ldots, \mathfrak{F}_n >$. Ils se calculent naturellement par factorisations successives de f dans les extensions k_i.

$\sigma^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}} = \mathfrak{M}_{\boldsymbol{\alpha}^{\sigma}} = \mathrm{Id}(\boldsymbol{\alpha}^{\sigma})$ (19); $\mathrm{Gal}_k(\boldsymbol{\alpha}^{\sigma}) = \sigma^{-1}\,\mathrm{Gal}_k(\boldsymbol{\alpha})\,\sigma$ (20); $\mathrm{V}(\mathfrak{M}_{\boldsymbol{\alpha}^{\sigma}}) = (\mathrm{Gal}_k(\boldsymbol{\alpha})\,\sigma) \star \boldsymbol{\alpha}$ (21)

IDEAL DES RELATIONS SYMETRIQUES : $\mathfrak{S} := \mathrm{Id}_k(\mathrm{S}_n \star \boldsymbol{\alpha})$.

$$\mathrm{V}(\mathfrak{S}) = \mathrm{S}_n \star \boldsymbol{\alpha} = \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \mid \sigma \in \mathrm{S}_n\} \quad .$$

$$\mathfrak{S} = < \mathrm{C}_1, \ldots, \mathrm{C}_n > .$$

où $\mathrm{C}_1(f), \ldots, \mathrm{C}_n(f)$ sont *les modules de Cauchy de* f dans $k[\boldsymbol{x}]$:

$$\mathrm{C}_r(x_r, \ldots, x_n) \quad := \quad \frac{\mathrm{C}_{r+1}(x_r, x_{r+2}, \ldots, , x_n) - \mathrm{C}_{r+1}(x_{r+1}, x_{r+2}, \ldots, , x_n)}{x_r - x_{r+1}} \quad 1 \leq r < n$$

Pour tout $\boldsymbol{\beta} \in \mathrm{V}(\mathfrak{S})$:

$$\begin{aligned}
\mathrm{C}_n(x_n) = f(x_n) &= (x_n - \beta_1)(x_n - \beta_2) \cdots (x_n - \beta_{n-1})(x_n - \beta_n) \qquad (6)\\
\mathrm{C}_{n-1}(x_{n-1}, \beta_n) &= (x_{n-1} - \beta_1)(x_{n-1} - \beta_2) \cdots (x_{n-1} - \beta_{n-1})\\
&\vdots\\
\mathrm{C}_r(x_r, \beta_{r+1}, \ldots, \beta_{n-1}, \beta_n) &= (x_r - \beta_1) \cdots (x_r - \beta_r)\\
&\vdots\\
\mathrm{C}_1(x_1, \beta_2, \ldots, \beta_n) &= x_1 - \beta_1 \quad .
\end{aligned}$$

Les n polynômes $\mathcal{V}_r := \sum_{i=0}^{r} a_i h_{r-i}(x_r, \ldots, x_n)$, $r \in [\![1, n]\!]$, satisfont ces n identités :

$$\mathrm{C}_r = \mathcal{V}_r \quad r = 1, \ldots, n \qquad (8)$$

Forme effective du théorème fondamental des fonctions symétriques :

$s \in k[\boldsymbol{x}]^{\mathrm{S}_n}$ polynôme symétrique, s réduit modulo $\{\mathrm{C}_1(x_1), \ldots, \mathrm{C}_n(x_n)\}$ via n divisions euclidiennes successives retourne $s(\alpha_1, \ldots, \alpha_n$.

IDEAUX GALOISIENS : $\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}} := \mathrm{Id}_k(\mathrm{L} \star \boldsymbol{\alpha})$

$\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}$ est l'*idéal galoisien défini par le couple* $(\mathrm{L}, \boldsymbol{\alpha})$ sur k.

$$\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{H}_1} \cap \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{H}_2} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{H}_1 \cup \mathrm{H}_2} \quad .$$

$$\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}} = \bigcap_{\sigma \in \mathrm{L}} \mathrm{Id}(\boldsymbol{\alpha}^{\sigma}) = \bigcap_{\sigma \in \mathrm{L}} \sigma^{-1} \cdot \mathfrak{M}_{\boldsymbol{\alpha}} \qquad (29)$$

Exprimer $\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}$ comme l'intersection d'idéaux comaximaux : voir Section 14.

$$\mathfrak{S} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{S}_n} \quad \subseteq \quad \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}} \quad \subseteq \quad \mathfrak{M}_{\boldsymbol{\alpha}} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{G}_{\boldsymbol{\alpha}}} \quad ,$$

ce qui induit les inclusions inverses suivantes sur les variétés :

$$\mathrm{G}_{\alpha} \star \boldsymbol{\alpha} \quad \subseteq \quad \mathrm{V}(\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}) \quad \subseteq \quad \mathrm{S}_n \star \boldsymbol{\alpha} \quad .$$

PROPOSITION 7 *Pour tout sous-ensemble* L *de* S_n *tel que* $\mathrm{I} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}$ *et où* $\mathrm{GL} := \{g\,l \mid g \in \mathrm{G}\,,\ l \in \mathrm{L}\}$.

$$\mathrm{V}(\mathrm{I}) = \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}}) \star \boldsymbol{\alpha} \quad \text{avec} \quad \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}}) = \mathrm{Gal}_k(\boldsymbol{\alpha})\mathrm{L} \qquad (30)$$

Les variétés galoisiennes irréductibles contenues dans V(I) sont les variétés $(\mathrm{Gal}_k(\boldsymbol{\alpha})\sigma) \star \boldsymbol{\alpha}$ où σ parcourt tout sous-ensemble L tel que $\mathrm{I} = \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}}$; ce qui en particulier est le cas pour $\mathrm{L} = \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}})$.

$$\chi_{\hat{\Theta},\mathrm{I}}(x) = \prod_{\boldsymbol{\beta} \in \mathrm{V}(\mathrm{I})} (x - \Theta(\boldsymbol{\beta})) = \prod_{\sigma \in \mathrm{Gal}_k(\boldsymbol{\alpha})\mathrm{L}} (x - \sigma \cdot \Theta(\boldsymbol{\alpha})) \quad \in k[x] \qquad (31)$$

Correspondance galoisienne : I et J galoisiens.

$$\mathfrak{S} \quad \subsetneq \quad \mathrm{I} \quad \subsetneq \quad \mathrm{J} \quad \subsetneq \quad \mathfrak{M}_{\boldsymbol{\alpha}} \quad \Rightarrow \quad \mathrm{S}_n \quad \supsetneq \quad \mathrm{Inj}(\mathrm{I}, \mathfrak{M}_{\boldsymbol{\alpha}}) \quad \supsetneq \quad \mathrm{Inj}(\mathrm{J}, \mathfrak{M}_{\boldsymbol{\alpha}}) \quad \supsetneq \quad \mathrm{G}_{\boldsymbol{\alpha}}$$
$$\mathrm{S}_n \quad \supsetneq \quad \mathrm{L} \quad \supsetneq \mathrm{H} \quad \Rightarrow \quad \mathfrak{S} \quad \subseteq \quad \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}} \quad \subseteq \quad \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{H}} \quad .$$

Si, de plus, $\boldsymbol{\alpha} \in \mathrm{V}(\mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{H}})$ (i.e. si L et H contiennent l'identité) alors

$$\mathfrak{S} \quad \subseteq \quad \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{L}} \quad \subseteq \quad \mathrm{I}_{\boldsymbol{\alpha}}^{\mathrm{H}} \quad \subseteq \quad \mathfrak{M}_{\boldsymbol{\alpha}} \quad .$$

Les inégalités sur les variétés galoisiennes s'ensuivent.

IDEAUX GALOSIENS PURS

On dit qu'un idéal galoisien I est un **pur** si $\mathrm{Inj}(I, \boldsymbol{\alpha}) = \mathrm{Stab}(I)$ pour tout $\boldsymbol{\alpha} \in V(I)$.

Il s'ensuit que dans toutes les formules l'ensemble de permutations $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}})$ peut être remplacé par le groupe Stab(I), avec $\boldsymbol{\alpha} \in V(I)$. En particulier : $V(I) = \mathrm{Stab}(I) \star \boldsymbol{\alpha}$.

Nous savons que pour tout idéal galoisien $I := Id_k(L \star \boldsymbol{\alpha})$ tel que $\boldsymbol{\alpha} \in V(I)$:

(i) $\mathrm{Inj}(I, M_{\boldsymbol{\alpha}})$ est, par définition, le plus grand ensemble qui définit I
(ii)

$$G_{\boldsymbol{\alpha}} \subset \mathrm{Inj}(I, M_{\boldsymbol{\alpha}})$$

(Correspondance galoisienne)
(iii) Puisque I est un idéal radical :

$$\mathrm{Card}(\mathrm{Inj}(I, M_{\boldsymbol{\alpha}})) = \mathrm{Card}(V(I)) = \dim_k k[\boldsymbol{x}]/I$$

Le stabilisateur Stab(I) de I contient tous les groupes définissant I avec $\boldsymbol{\alpha}$ d'après le lemme (13) suivant :

LEMME (13) Si $I \subseteq \mathfrak{M}_{\boldsymbol{\alpha}}$ alors Stab(I) contient tous les sous-groupes H du groupe symétrique S_n tels que $I = I_{\boldsymbol{\alpha}}^H$.

DÉMONSTRATION. Soit H un sous-groupe de S_n tel que $I = I_{\boldsymbol{\alpha}}^H$. Prenons $h \in H$ et $r \in I$. Nous savons que $h \cdot r \in I$ est équivalent à $\sigma \cdot (h \cdot r)(\boldsymbol{\alpha}) = 0$ pour tout $\sigma \in H$, par définition de $I_{\boldsymbol{\alpha}}^H$. Or puisque H est un groupe, $\sigma h \in H$ et, par conséquent, par définition de $I_{\boldsymbol{\alpha}}^H$, $0 = \sigma h \cdot r(\boldsymbol{\alpha}) = \sigma \cdot (h \cdot r)(\boldsymbol{\alpha})$. Donc $h \cdot r \in I$ et $h \in \mathrm{Stab}(I)$. □

L'idéal I est pur lorsque Stab(I) contient lui aussi le groupe de Galois $G_{\boldsymbol{\alpha}}$, pour $\boldsymbol{\alpha} \in V(I)$.

L'idéal des relations symétriques et tous les maximaux de relations sont purs. Ils sont triangulaires. Au cours 11, vous démontrerez que tous les idéaux galoisiens purs sont triangulaires.

On vérifie qu'un idéal galoisien triangulaire I est pur en testant si le cardinal de Stab(I), calculable avec des divisions euclidiennes, est identique à celui $\mathrm{Inj}(I, \boldsymbol{\alpha})$, produit des degrés initiaux de l'ensemble triangulaire qui engendre I (voir cours 12).