CALCUL ALGÉBRIQUE - UE 4M021

MASTER 1 MATHS - FACULTÉ DES SCIENCES - SORBONNE UNIVERSITÉ

Annick Valibouze

2017-2018

TD 10

Rappels de cours : Nous avons défini l'injecteur d'un idéal I dans un idéal J : $\mathrm{Inj}(I,J) := \{\sigma \in S_n \mid \sigma \cdot I \subset J\}$ et le stabilisateur de I : $\mathrm{Stab}(I) := \mathrm{Inj}(I,I)$. Soit $f \in \mathbb{Q}[x]$ séparable (i.e. racines deux-à-deux distinctes) de degré n et $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n)$ un n-uplet de ses racines. Pour un idéal dit galoisien $I := \mathrm{Id}(L \star \boldsymbol{\alpha})$ nous avons $\mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}}) = G_{\boldsymbol{\alpha}} L$ et $V(I) := \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}}) \star \boldsymbol{\alpha}$. Deux idéaux galoisiens particuliers : $\mathfrak{S} := \mathrm{Id}(S_n \star \boldsymbol{\alpha})$ est l'idéal des relations symétriques et $\mathfrak{M}_{\boldsymbol{\alpha}} := \mathrm{Id}(\boldsymbol{\alpha})$ (idéal maximal car d'un point, avec $L = I_n$) est l'idéal des $\boldsymbol{\alpha}$-relations. Pour tout $\boldsymbol{\beta} \in V(I)$, nous avons l'intersection d'idéaux maximaux galoisiens (non nécessairement distincts) suivante :

$$I = \bigcap_{\boldsymbol{\beta} \in V(I)} \mathfrak{M}_{\boldsymbol{\beta}}$$

avec $V(\mathfrak{M}_{\boldsymbol{\beta}}) = G_{\boldsymbol{\beta}} \star \boldsymbol{\beta}$ (cas trivial lorsque $L = I_n$). Lorsque L est un groupe et qu'il contient $G_{\boldsymbol{\alpha}} = \mathrm{Stab}(\mathfrak{M}_{\boldsymbol{\alpha}})$, l'idéal galoisien $I := \mathrm{Id}(L \star \boldsymbol{\alpha})$ est dit pur et $V(I) := L \star \boldsymbol{\alpha} = L \star \boldsymbol{\beta}$ pour tout $\boldsymbol{\beta} \in V(I)$, avec $\mathrm{Stab}(I) = \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}}) = L$. Les idéaux $\mathfrak{S} := \mathrm{Id}(S_n \star \boldsymbol{\alpha})$ et $\mathfrak{M}_{\boldsymbol{\alpha}} := \mathrm{Id}(\boldsymbol{\alpha})$ sont purs puisque pour chacun, si $\boldsymbol{\alpha}$ est dans sa variété alors son stabilisateur s'identifie à son injecteur dans l'idéal des $\boldsymbol{\alpha}$-relations : $S_n = \mathrm{Stab}(\mathfrak{S}) = \mathrm{Inj}(\mathfrak{S}, \mathfrak{M}_{\boldsymbol{\alpha}})$ et pour $L = I_n$, $G_{\boldsymbol{\alpha}} = \mathrm{Stab}(\mathfrak{M}_{\boldsymbol{\alpha}}) = \mathrm{Inj}(\mathfrak{M}_{\boldsymbol{\alpha}}, \mathfrak{M}_{\boldsymbol{\alpha}})$.

EXERCICE 1

Soit $f(x) = (x-3)(x-5) = x^2 - 8x + 15$ et $k = \mathbb{Q}$.

Question 1.1 Donner des générateurs de l'idéal des relations symétriques $\mathfrak{S}$ à partir des fonctions symétriques élémentaires. (Indication : se reporter à la démonstration de $V(\mathfrak{S}) = S_n \star \boldsymbol{\alpha}$.)

Question 1.2 Donner un ensemble triangulaire $\{C_1(x_1, x_2), C_2(x_2)\}$ qui engendre $\mathfrak{S}$. Pourquoi est-il bien séparable ?

Question 1.3 Soit la fonction symétrique $s(x_1, x_2) := x_1^2 x_2 + x_2^2 x_1$. Notons r_1, le reste de la division euclidienne de s par C_1 en x_1 et r_2 celui de r_1 par C_2 en x_2. Que remarquez-vous ?

Question 1.4 Donner la variété $V(\mathfrak{S})$ et l'arbre de cette variété.

Question 1.5 Fixons $\boldsymbol{\alpha} = (\alpha_1 = 3, \alpha_2 = 5)$. Considérer la $\boldsymbol{\alpha}$-relation $x_1 - 3$ (on a bien $\alpha_1 - 3 = 0$). Le groupe de Galois $G_{(\alpha_1,\alpha_2)}$ est-il identique au groupe symétrique S_2 ?

Question 1.6 Si $G_{(\alpha_1,\alpha_2)} \neq S_2$, donner les idéaux maximaux $\mathfrak{M}_{\mathfrak{b}}$ distincts contenant $\mathfrak{S}$, leurs stabilisateurs respectifs $G_{\mathfrak{b}}$ ainsi que les arbres de leurs variétés respectives. A-t-on $G_{(\alpha_1,\alpha_2)} \neq G_{(\alpha_2,\alpha_1)}$?

EXERCICE 2

Soit $f(x) = (x-i)(x+i) = x^2+1$.

Question 2.1 Refaire les questions 1,2,3,4 de l'Exercice 1.

Question 2.2 A-t-on $G_{(\alpha_1,\alpha_2)} = S_2$? Pourquoi ?

Question 2.3 Que calcule

$$R := \mathrm{Res}_{x_2}(C_2(x_2), \mathrm{Res}_{x_1}(C_1(x_1,x_2), x-(x_1-x_2))) \quad ?$$

Question 2.4 Remplacer $x_1 - x_2$ par $p(x_1,x_2)$. Montrer que $R = \chi_{p,\mathfrak{S}}$, le polynôme caractéristique de l'endomorphisme multiplicatif $\hat{p}$ induit p dans $\mathbb{Q}[x_1,x_2]/\mathfrak{S}$. Soit $\gamma = p(\alpha_1,\alpha_2)$. Constater que $\min_{\gamma,\mathbb{Q}}$ est un facteur de R.

Question 2.5 Soient $a,b,p \in k[\boldsymbol{x}]$ avec $a \neq 0$ et b de degré 0 en x_1. Remarquez que $\mathrm{Res}_{x_1}(ax_1+b, y-p(\boldsymbol{x})) = y - p(-b/a, x_2, \ldots x_n)$? Qu'en concluez-vous ?

Question 2.6 Pourquoi R est un carré dans $\mathbb{Q}$ avec $p(x_1,x_2) = x_1^2 + x_2^2$? Est-ce le cas chaque fois que p est symétrique en x_1, x_2 ?

Question 2.7 Que calcule $\mathrm{Res}_{x_2}(f(x_2), \mathrm{Res}_{x_1}(f(x_1), x-(x_1-x_2)))$? Qu'en concluez-vous ?

EXERCICE 3

Soit $f(x) = x^3+1 = (x+1)(x^2-x+1)$; nous savons que les racines sont $\alpha_1 = -1, \alpha_2 = e^{i\pi/3}, \overline{\alpha_2}$.

Question 3.1 Donner un ensemble triangulaire engendrant l'idéal des relations symétriques de f.

Question 3.2 Soit $\boldsymbol{\alpha} = (\alpha_1 = -1, \alpha_2, \alpha_3)$ un n-uplet des 3 racines de f. Soit la $\boldsymbol{\alpha}$-relation $r = x_2^3 - x_1$. Trouver $\tau \in S_3$ qui n'envoie pas r dans $Id(\boldsymbol{\alpha})$. Le groupe de Galois est-il S_3 ?

Question 3.3 Donner un ensemble triangulaire engendrant l'idéal maximal $Id(\boldsymbol{\alpha})$. Donnez les éléments du groupe de Galois $G := G_{\boldsymbol{\alpha}}$.

Question 3.4 Vérifier que $\{(1)(2)(3),(1,2),(1,3)\}$ est une transversale à droite de G mod S_3. Combien d'idéaux co-maximaux contiennent $\mathfrak{S}$? Pouvez-vous les exprimer à partir de $Id(\boldsymbol{\alpha})$? Donner leurs générateurs respectifs.

EXERCICE 4

Soit $f \in k[x]$ un polynôme de degré n de racines deux-à-deux distinctes $\alpha_1, \alpha_2, \ldots, \alpha_n$ et $\phi \in k[\boldsymbol{x}]$. (Les questions 4.1, 4.2 et 4.3 ont normalement été traitées au TD 9 dans un cas plus général).

Question 4.1 Soit $r_0 = \phi$ et pour $i = 1, \ldots, n$, soit r_i le reste de la division de r_{i-1} par C_i en x_i. Montrez qu'en divisant ainsi successivement ϕ par les termes de la suite des modules de Cauchy $C_1(x_1, \ldots, x_n), \ldots, C_n(x_n)$, le degré du dernier reste r_n en la variable x_i est strictement inférieur au degré i de C_i en x_i.

Question 4.2 Soit $r \in k[\boldsymbol{x}]$. Montrer que si r satisfait les conditions suivantes :
(i) r est une relation symétrique
(ii) pour tout $j \in [\![1, n]\!]$ $\deg_{x_j}(r) < \deg_{x_j}(C_j) = j$
alors $r = 0$.

Question 4.3 Sous les hypothèse de la question (1), le polynôme ϕ est une relation symétrique en les racines de f si et seulement si le dernier reste r_n est nul.

Question 4.4 Pouvez-vous proposer une méthode pour calculer la valeur dans $\mathbb{Q}$ de tout polynôme symétrique s en $\alpha_1, \alpha_2, \ldots, \alpha_n$ à coefficients dans $\mathbb{Q}$? (En remarquant que $s(\boldsymbol{x}) - s(\boldsymbol{\alpha}) \in \mathfrak{S}$.) Cette méthode est due à Augustin Cauchy.

EXERCICE 5

Soit le polynôme $f(x) = x^6 + 2$ irréductible sur $\mathbb{Q}$ (pouvez-vous le vérifier ?). Nous supposons que le groupe de Galois de f est inclus dans "le" groupe dihédral de degré 6 et d'ordre 12. Soit ce groupe dihédral $L := D_6 :=< (1,2)(3,4)(5,6), (1,5,3)(2,6,4), (1,3)(2,4) >$ définissant un idéal galoisien I de f. Nous nous proposons de montrer que ces polynômes :

$$f_1 := x_1 - x_4 - x_6, f_2 := x_2 + x_4 + x_6, f_3 := x_3 + x_4, f_4 := x_4^2 + x_4 x_6 + x_6^2, f_5 := x_5 + x_6, f_6 := x_6^6 + 2$$

engendrent un idéal galoisien pur de f de stabilisateur D_6. Nous supposons que pour toute racine α de f, les polynômes $x + \alpha$ et $x^2 + \alpha x + \alpha^2$ sont des facteurs de f sur son corps de rupture $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/f(x)$. Vous pouvez le vérifier en `Maxima` avec la commande `factor(x^6+2,y^6+2)`.

Question 5.1 Pourquoi l'idéal galoisien I est-il pur ? Nous supposons savoir que dans ce cas, I est triangulaire ; ce qui signifie que I est engendré par un ensemble triangulaire séparable $\{f_1(x_1, \ldots, x_6), \ldots, f_6(x_6)\}$ (voir TD 11).

Question 5.2 Posons $d_i := \deg_{x_i} f_i$. Nous supposons savoir que $d_i = 1$ pour $i = 1,2,3,5$ et $d_6 = 6$ (voir TD 11). Pourquoi $d_4 = 2$?

Question 5.3 Soit $\boldsymbol{\beta} \in \mathrm{V(I)}$. On voudrait choisir $f_5 = x_5 + x_6$ qui correspondrait au facteur $x + \beta_6$ sur $\mathbb{Q}(\beta_6)$. Pour que $x_5 + x_6$ appartienne à I, quelle relation choisir alors pour f_3 ?

Question 5.4 Avec le facteur $x^2 + \alpha x + \alpha^2$, pouvez-vous choisir $f_4 = x_4^2 + x_4 x_6 + x_6^2$?

Question 5.5 En vous servant des fonctions symétriques des racines de $\mathrm{F}_4 = x_4^2 + \beta_6 x_4 + \beta_6^2$, que serait alors f_2 ? Cela se vérifie-t-il avec les générateurs de D_6 ?

Question 5.6 Nous savons que $x_1 + \cdots + x_6 - (\beta_1 + \cdots + \beta_6) = x_1 + \cdots + x_6 \in \mathrm{I}$ pourrait convenir pour f_1. Le polynôme $f_1 = x_1 - x_4 - x_6$ en serait-il une forme "réduite" mod I?

Question 5.7 Comment vérifier que vous avez bien obtenu les générateurs triangulaires réduits de I ? Faites-le.

EXERCICE 6 (Pour les plus rapides)

Montrer que si un polynôme $p \in \mathbb{Q}[\boldsymbol{x}]$ est stabilisé par L (i.e. p est un L-invariant) où I est d'injecteur L alors $p(\boldsymbol{x}) - p(\boldsymbol{\alpha}) \in \mathrm{I}$. Remarquer que la réduction r de p mod I appartient à $\mathbb{Q}$. Montrer que si $\Theta \in \mathbb{Q}[\boldsymbol{x}]$, et L un sous-groupe de S_n alors tout polynôme symétrique en les éléments de l'orbite $\mathrm{L}\cdot\Theta$ (par exemple, la somme des $\Psi(\boldsymbol{x})$ dans $\mathrm{L}\cdot\Theta$) est un polynôme p de $\mathbb{Q}[\boldsymbol{x}]^{\mathrm{L}}$ (i.e. invariant pat l'action de L sur $x_1, \ldots, x_n$). En déduire lorsque L est un groupe contenant $\mathrm{G}_{\boldsymbol{\alpha}}$, on a $p(\alpha) \in \mathbb{Q}$. En déduire que ce polynôme a ses coefficients dans $\mathbb{Q}$:

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

Ce polynôme s'appelle la résolvante de I par Θ. En déduire un algorithme qui calcule la résolvante $\mathrm{R}_{\Theta,\mathrm{I}}$ lorsque l'idéal galoisien I est donné par un ensemble triangulaire séparable l'engendrant.

CALCUL ALGÉBRIQUE - UE 4M021
MASTER 1 MATHS - FACULTÉ DES SCIENCES - SORBONNE UNIVERSITÉ

Annick Valibouze
2017-2018

TD 11

Rappels de cours : Soit I in idéal galoisien et $L = \mathrm{Inj}(I, \mathfrak{M}_{\boldsymbol{\alpha}}$. Le polynôme d'une variable

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

ne dépend pas du choix de $\boldsymbol{\alpha}$ dans V(I). Il est appelé la I-résolvante par Θ.
Un idéal galoisien pur est triangulaire. Fixons I est un idéal galoisien pur.
Pour tout $\boldsymbol{\beta} \in V(I)$, nous avons comme pour les modules de Cauchy, $F_n := f_n$ et pour chaque $r \in [\![1, n-1]\!]$:

$$F_r(x_r) := f_r(x_r, \beta_{r+1}, \ldots, \beta_{n-1}, \beta_n) = (x_r - \beta_{\sigma_1(r)})(x_r - \beta_{\sigma_2(r)}) \cdots (x_n - \beta_{\sigma_{d_r}(r)}) \quad (1)$$

où $L_{n+1} := L$, $L_{(r+1)} = \sigma_1 L_{(r)} + \cdots + \sigma_{d_r} L_{(r)}$ avec $\sigma_{d_r} = id$ et $L_{(r)} := \{\sigma \in L_{(r+1)} \mid \sigma(r) = r\}$.

L'ensemble $T_r := \{\sigma_1, \ldots, \sigma_{d_r}\}$ est une transversale à gauche de $L_{(r+1)} \mod L_{(r)}$ de cardinal $d_r = \deg_{x_r} f_r$. Si H est un groupe alors la transversale de $H \mod \mathrm{Stab}_H(r)$ est appelée aussi la transversale de r dans H. Par exemple, le logiciel `SageMath` manipulant les groupes la calcule avec la commande `H.transversale(r)`. De même `H.stabiliser(r)` calcule $\mathrm{Stab}_H(r)$.

Nous disposons de tous les moyens pour décrire un idéal galoisien pur à partir de son groupe de décomposition. L'objectif de cet exercice est de le faire sur une exemple.

EXERCICE 1

Soit le polynôme $f(x) = x^6 + 2$ irréductible sur $\mathbb{Q}$ (voir TD 10). Nous supposons savoir que le groupe de Galois de f est inclus dans "le" groupe dihédral de degré 6 et d'ordre 12. Soit ce groupe dihédral $L := D_6 :=< (1,2)(3,4)(5,6), (1,5,3)(2,6,4), (1,3)(2,4) >$ définissant un idéal galoisien I de f. Un calcul rapide dans le logiciel `SageMath` fournit les informations suivantes : en posant, $L_{(7)} = L = D_6$, nous obtenons :

$$L_{(6)} = L_{(5)} = \{Id, (1,3)(2,4)\} \text{ et } L_{(4)} = L_{(3)} = L_{(2)} = L_{(1)} = \{id\} \quad .$$

Pour décrire l'arbre de la variété, nous utilisons :
$L_{(6)}/L_{(5)} = L_{(4)}/L_{(3)} = L_{(3)}/L_{(2)} = L_{(2)}/L_{(1)} = \{id\}$, $L_{(5)}/L_{(4)} = L_{(5)}$ et

$$L_{(7)}/L_{(6)} = \{id, (3,5)(4,6), (1,2)(3,4)(5,6), (1,2)(3,6)(4,5), (1,3,5)(2,4,6), (1,4,5,2,3,6))$$

Question 1.1 Pourquoi l'idéal galoisien I est-il engendré par un ensemble triangulaire séparable $\{f_1(x_1, \ldots, x_6), \ldots, f_6(x_6)\}$. Nous supposons cet ensemble réduit.

Question 1.2 A partir des $L_{(i)}$, donnez les formes des polynômes f_i et F_i pour $\boldsymbol{\beta}$ dans V(I). En particulier, donnez les degrés de chaque polynôme f_i en chaque variable x_j.

Question 1.3 Dessinez l'arbre de la variété de I.

EXERCICE 2

Poursuivons avec notre polynôme $f = x^6 + 2$. Nous voulons montrer que l'idéal I est maximal ; i.e. D_6 est le groupe de Galois de tout $\boldsymbol{\alpha} \in V(I)$. Les polynôme "réduits" de l'ensemble triangulaire engendrant I notre idéal galoisien pur de f sont :

$$f_1 = x_1 - x_4 - x_6, f_2 = x_2 + x_4 + x_6, f_3 = x_3 + x_4, f_4 = x_4^2 + x_4x_6 + x_6^2, f_5 = x_5 + x_6, f_6 = x_6^6 + 2$$

et son stabilisateur est D_6. Soit $C_6 :=< (1,2)(3,4)(5,6), (1,3,5)(2,4,6) >$ un des deux sous-groupes cycliques de $D_6 = C_6 + \sigma C_6$ où $\sigma = (3,5)(4,6)$ (i.e. le conjugué de C_6 dans D_6 est $\sigma C_6 \sigma^{-1}$) et soit

$$P = x_5x_4^2 + x_6x_3^2 + x_2x_5^2 + x_3x_2^2 + x_1x_6^2 + x_4x_1^2$$

tel que $\mathrm{Stab}_{D_6}(P) = C_6$; i.e. un C_6-invariant D_6-primitif.

Question 2.1 En vous servant de l'expression du polynôme minimal sur $\mathbb{Q}$ (Théorème de Galois), montrez que f est irréductible si et seulement si tout conjugué G de groupe de Galois est transitif ; i.e. pour tout couple i, j dans $[\![1, n]\!]$ il existe $g \in G$ tel que $g(i) = j$. (Devoir - nous l'admettrons)

Question 2.2 Le groupe de Galois de f peut-il être un sous-groupe propre de C_6 ?

Question 2.3 En déduire les deux groupes de Galois possibles pour $f = x^6 + 2$.

Question 2.4 Quel est le degré de la résolvante $R_{P,I}$? Quelles sont ses racines (formellement).

Question 2.5 Calculer les réductions modulo I des éléments de l'orbite $D_6 \cdot P$. Qu'en concluez-vous ?

Question 2.6 Soit $g(y) \in \mathbb{Q}[y]$, un polynôme non constant et $\Theta = P(g(x_1), \ldots, g(x_6))$. Nous avons $\mathrm{Stab}_{D_6}(P) = C_6$. Nous cherchons g tel que $\Theta(\boldsymbol{\alpha})$ soit une racine simple de $R_{\Theta,I}$. Pourquoi ?

Question 2.7 Soit $g = x^2$. Notons Θ' l'autre élément de l'orbite de Θ. Avec les mêmes calculs qu'en 2.4, nous trouvons que $[\Theta] = 6x_4x_6^5 + 6$ et $[\Theta'] = -6x_4x_6^5 + 18$. Soit $r := \Theta - \Theta'$. En vous servant des générateurs de I, montrer que $r(\boldsymbol{\alpha}) \neq 0$.

Question 2.8 Calculer $R_{\Theta,I}$. Qu'en concluez-vous ?

CALCUL ALGÉBRIQUE - UE 4M021
MASTER 1 MATHS - FACULTÉ DES SCIENCES - SORBONNE UNIVERSITÉ

Annick Valibouze
2017-2018

TD 12

EXERCICE 1

Soit le polynôme $f = x^8+x^4+2$ irréductible sur $\mathbb{Q}$. Soit M un sous-groupe transitif de S_8 d'ordre 1152. Soit $P = x_1x_2x_3x_4+x_5x_6x_7x_8$ tel que $\mathrm{Stab}_{S_8}(P) = M$. Soit H un sous-groupe de M d'ordre 128 et $\Theta == x_1x_2+x_3x_4+x_5x_6+x_7x_8$ un M-invariant H-primitif. Et soit G un sous-groupe d'indice 2 dans H d'invariant Ψ dans H.

Question 1.1 La résolvante $R_{P,\mathfrak{S}} = (x-1)x^8(x^2-8)^5(x^4-8x^2+14)^4$ possède une racine simple dans $\mathbb{Q}$. Qu'en concluez-vous ?

Question 1.2 Soit $I = I_{\boldsymbol{\alpha}}^{M}$ l'idéal galoisien du 1. Nous trouvons 3 idéaux triangulaires J_1, J_2, J_3 tels que pour chacun le produit des degrés initiaux est 384 et $I = J_1 \cap J_2 \cap J_3$. Qu'en concluez-vous ? Par exemple :

$$\begin{aligned} J_1 \;=\; \langle & x_1^8+x_1^4+2,\ x_2+x_1,\ x_3^2+x_1^2,\ x_4+x_3,\ x_5^4+x_1^4+1,\ x_6^3+x_6^2x_5+x_6x_5^2+x_5^3, \\ & x_7^2+x_7x_6+x_7x_5+x_6^2+x_6x_5+x_5^2,\ x_8+x_7+x_6+x_5\rangle\ . \end{aligned}$$

Question 1.3 Par la méthode des résultants combien des 8 résultants pourriez-vous éviter pour calculer R_{Θ,J_1} ? Quel est le degré du polynôme que vous obtenez à la fin du calcul ?

Question 1.4 Les calculs fournissent ci-dessous les polynômes minimaux des 3 endomorphismes induits par Θ (i.e. les formes sans facteur carré des polynômes caractéristiques). En déduire la résolvante $R_{\Theta,I}$. Qu'en concluez-vous ?

$$\begin{aligned} M_{\Theta,J_1} &= x(x^4-4x^2+32) \quad \text{et} \\ M_{\Theta,J_2} &= M_{\Theta,J_3} = (x^4-4x^2+32)(x^4-8x^2-112) \end{aligned}$$

Question 1.5 En utilisant la permutation $\tau := (1,5)(2,6)(3,7)(4,8)$ de H, retrouvez cet ensemble triangulaire engendrant $J := I_{\boldsymbol{\alpha}}^{H}$

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

Question 1.6 La réduction de Ψ modulo J est $\Psi' = 128x_1^3x_3x_5^3x_7 + 352$. En calculant $R_{\Psi,J} = R_{\Psi',J}$, nous trouvons $(x-96)(x+608)$. Qu'en concluez-vous ? Pouvez-vous en déduire $I_{\boldsymbol{\alpha}}^G$?

Question 1.7 Le discriminant de f est $2^{19}7^4$. Qu'en concluez-vous ?

Pour conclure, en calculant une résolvante par un invariant de la seule classe de conjugaison dans G qui pourrait être celle du groupe de Galois (pourquoi à votre avis ?), nous ne trouvons aucune racine dans $\mathbb{Q}$. Donc le groupe de Galois est bien G. Le calcul avec des techniques qui dépassent le cadre de ce cours aboutissent à l'ensemble triangulaire suivant qui engendre un idéal maximal $I_{\boldsymbol{\alpha}}^G$:

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

Ces techniques peuvent faire appel à la factorisation dans les extensions (voir Exercice 5 TD10) ou à d'autres comme celles dites des bases de Gröbner.

Corrigé TD 10 - Annick Valibouze

Nous donnons ici un corrigé très détaillé pour assimiler sur des exemples simples les principales notions du cours 10 et préparer aux cours suivants.

Exercice 1 Soit $f(x) = (x-3)(x-5) = x^2 - 8x + 15$ et $k = \mathbb{Q}$.

1.1 Donner des générateurs de l'idéal des relations symétriques $\mathfrak{S}$ à partir des fonctions symétriques élémentaires. (Indication : se reporter à la démonstration de $V(\mathfrak{S}) = S_n \star \boldsymbol{\alpha}$.)

Réponse. D'après le cours, pour n-uplet $\boldsymbol{\alpha}$ des racines de f : $\mathfrak{S} =< e_1(\boldsymbol{x}) - e_1(\boldsymbol{\alpha}), e_2(\boldsymbol{x}) - e_2(\boldsymbol{\alpha}) >$ où e_i est la i-ième fonction symétrique élémentaire. Rappelons que pour un polynôme unitaire quelconque de degré n et de racines $\beta_1, \ldots \beta_n$, le coefficient de x^{n-i} dans ce polynôme est $(-1)^i e_i(\beta_1, \ldots, \beta_n)$. Ici, même sans cela, nous voyons que : $e_1(3,5) = 8 = 3+5$ et $e_2 = 15 = 3 \times 5$. D'où $\mathfrak{S} =< x_1 + x_2 - 8, x_1 x_2 - 15 >$.

1.2 Donner un ensemble triangulaire $\{C_1(x_1, x_2), C_2(x_2)\}$ qui engendre $\mathfrak{S}$. Pourquoi est-il bien séparable ?

Réponse. D'après le cours, on peut prendre les modules de Cauchy : $C_2(x_2) := f_2(x_2) = x_2^2 - 8x_2 + 15$ et sans même utiliser la formule (3.5) $C_r = \mathcal{V}_r$, le premier module de Cauchy est donné par :

$$C_1(x_1, x_2) := \frac{(x_1^2 - 8x_1 + 15) - (x_2^2 - 8x_2 + 15)}{x_1 - x_2} = x_1 + x_2 - 8 \quad .$$

Nous retrouvons tout naturellement : $C_1(\boldsymbol{x}) = e_1(\boldsymbol{x}) - e_1(\boldsymbol{\alpha}) = e_1(\boldsymbol{x}) + \text{Coeff}(f, x, n-1)$ où n est le degré de f. L'ensemble triangulaire $\{C_1, C_2\}$ est bien séparable car $C_2(x_2)$ n'a pas de racine multiple et, pour chacune de ses racines 5 et 3, ni $C_1(x_1, 3) = x - 5$ ni $C_1(x_1, 5) = x - 3$ n'ont de racine multiple.

1.3 Soit la fonction symétrique $s(x_1, x_2) := x_1^2 x_2 + x_2^2 x_1$. Notons r_1, le reste de la division euclidienne de s par C_1 en x_1 et r_2 celui de r_1 par C_2 en x_2. Que remarquez-vous ?

Réponse. Divisons s par C_1 en x_1 : $x_1^2 x_2 + x_2^2 x_1 = (x_1 x_2 + 8x_2)C_1 + 64x_2 - 8x_2^2$; on peut le faire "à la main" ou avec la commande `maxima` suivante :
`divide(x1**2*x2 +x2**2*x1,x1+x2-8,x1);`
qui retourne la liste `[x1*x2+8*x2,64*x2-8*x2**2]` du quotient et du reste. D'où

$$r_1 = 64x_2 - 8x_2^2 = -8(x_2^2 - 8x_2) = -8C_2(x_2) + 8 \times 15 = -8C_2(x_2) + 120 \quad .$$

Ainsi $r_2 = 120 \in \mathbb{Q}$, le corps des coefficients $\mathbb{Q}$ de f. On dira que 120 est la **réduction de s modulo** $< C_1, C_2 >$. Comme $s(x_1, x_2) = q_2 C_2(x_2) + q_1 C_1(x_1, x_2) + 120$, le polynôme $s(x_1, x_2) - 120$ est une relation symétrique (entre les racines de f), avec, en particulier,

$s(\alpha_1,\alpha_2) = 120$. Notons qu'ici, nous pouvons vérifier "à la main" que $s(3,5) = s(5,3) = 120$.

1.4 Donner la variété $V(\mathfrak{S})$ et l'arbre de cette variété.

Réponse. Pour construire $V(\mathfrak{S})$, puisque l'idéal est triangulaire, on part de chacune des racines a_2 de $C_2(x_2)$ et on récolte la racine a_1 de $C_1(x_1,a_2)$ (une seule racine car C_1 de degré 1 en x_1). Cela se généralise en tout degré n. On obtient ainsi tous les points (a_1,a_2) de la variété. L'arbre de la variété est composé des chemins $o \to a_2 \to a_1$ où o est la racine de l'arbre (que l'on peut oublier). Pour $a_2 = 3$, $C_1(x_1,3) = x_1 - 5$ a pour racine $a_1 = 5$; d'où $(5,3) \in V(\mathfrak{S})$. En partant de l'autre racine $a_2 = 5$ de C_2, nous avons $C_1(x_1,5) = x_1 - 3$; d'où $(3,5) \in V(\mathfrak{S})$. Nous avons balayé tous les zéros de $\mathfrak{S}$ et donc $V(\mathfrak{S}) = \{(3,5),(5,3)\}$. L'arbre de la variété est composé des deux branches suivantes : $3 \to 5$ et $5 \to 3$.

Commentaire. Notons que retrouvons bien que l'ensemble des solutions est la permutation par le groupe symétrique S_2 d'un 2-uplet quelconque des racines de f : $V(\mathfrak{S}) = S_n \star \boldsymbol{\alpha}$.

1.5 Fixons $\boldsymbol{\alpha} = (\alpha_1 = 3, \alpha_2 = 5)$. Considérer la $\boldsymbol{\alpha}$-relation $x_1 - 3$ (on a bien $\alpha_1 - 3 = 0$). Le groupe de Galois $G_{(\alpha_1,\alpha_2)}$ est-il identique au groupe symétrique S_2 ?

Réponse. Puisque $r = x_1 - 3$ est une $\boldsymbol{\alpha}$-relation, toute permutation τ du groupe de Galois envoie r vers une autre $\boldsymbol{\alpha}$-relation. Avec $\tau = (1,2)$, nous avons $\tau \cdot r = x_2 - 3$; si on évalue $\tau \cdot r$ en $\boldsymbol{\alpha} = (3,5)$, on obtient $5 - 3 \neq 0$. Donc $\tau \cdot r$ n'est pas une $\boldsymbol{\alpha}$-relation et $\tau \notin G_{(\alpha_1,\alpha_2)} \neq S_2$.

1.6 Si $G_{(\alpha_1,\alpha_2)} \neq S_2$, donner les idéaux maximaux $\mathfrak{M}_{\boldsymbol{\beta}}$ distincts contenant $\mathfrak{S}$, leurs stabilisateurs respectifs $G_{\boldsymbol{\beta}}$ ainsi que les arbres de leurs variétés respectives. A-t-on $G_{(\alpha_1,\alpha_2)} \neq G_{(\alpha_2,\alpha_1)}$?

Réponse. $\mathfrak{M}_{(3,5)} =< x_1 - 3, x_2 - 5 >$, $G_{(3,5)} = I_2$, $V(\mathfrak{M}_{(3,5)}) = \{(3,5)\}$, arbre : $5 \to 3$ et de même $\mathfrak{M}_{(5,3)} =< x_1 - 5, x_2 - 3 >$, $G_{(5,3)} = I_2$, $V(\mathfrak{M}_{(5,3)}) = \{(5,3)\}$, arbre : $3 \to 5$. Les stabilisateurs respectifs des deux idéaux co-maximaux $\mathfrak{M}_{(3,5)}$ et $\mathfrak{M}_{(5,3)}$ contenant $\mathfrak{S}$ sont identiques : $G_{(3,5)} = G_{(5,3)} = I_2$. Les groupes de Galois sont identiques car le groupe identité est un sous-groupe distingué du groupe symétrique. .

Commentaire. Nous retrouvons l'union disjointe de variétés (irréductibles) $V(\mathfrak{S}) = V(\mathfrak{M}_{(3,5)}) \cup V(\mathfrak{M}_{(5,3)})$ et $\mathfrak{S} = \mathfrak{M}_{(3,5)} \cap \mathfrak{M}_{(5,3)}$ (voir cours). En posant $\tau = (1,2) \in S_2$, nous avons $S_2 = G_{(3,5)} + G_{(3,5)}\tau = \{I_2, \tau\}$; puisque $(5,3) = (3,5)^\tau$ on a $\mathfrak{M}_{(5,3)} = \mathrm{Id}((3,5)^\tau) = \tau^{-1} \cdot \mathfrak{M}_{(3,5)}$ et $G_{(5,3)} = \tau \cdot G_{(3,5)} \tau^{-1} = G_{(3,5)} = I_2$.

Exercice 2 Soit $f(x)=(x-i)(x+i)=x^2+1$ et $\boldsymbol{\alpha}=(\alpha_1,\alpha_2)$, un n-uplet quelconque de ses 2 racines i et $-i$.

2.1 Refaire les questions 1,2,3,4 de l'Exercice 1.

Réponse. (1) $\mathfrak{S}=<x_1+x_2, x_1x_2-1>$. (2) $C_2(x_2)=f_2(x_2)=x_2^2+1$ et $C_1(x_1,x_2)=x_1+x_2$. (3)Nous avons $s(x_1,x_2):=x_1^2x_2+x_2^2x_1=x_1x_2C_1+0$. Donc le reste r_2 des divisions successives est nul. Il appartient à $\mathbb{Q}$. Ici s est une relation symétrique entre les racines de f. Comme dans l'Exercice 1, nous trouvons la valeur 0 dans $\mathbb{Q}$ du polynôme symétrique s évalué en les racines du polynôme x^2+1. (4) $V(\mathfrak{S})=\{(i,-i),(-i,i)\}$.

2.2 A-t-on $G_{(\alpha_1,\alpha_2)}=S_2$? Pourquoi ?

Réponse 1. Oui. Sinon, il existerait une $\boldsymbol{\alpha}$-relation non symétrique. Soit une (α_1,α_2)-relation $r(x_1,x_2)$. La division de $r(x_1,x_2)$ par C_1 en x_1, revient à remplacer x_1 par $-x_2$ dans r ; i.e. comme $\alpha_1=-\alpha_2$, on a $r(\alpha_1,\alpha_2)=r(-\alpha_2,\alpha_2)=0$ (voir [1]) . Soit $F(x_2)=r(-x_2,x_2)$; on a $F(\alpha_2)=r(-\alpha_2,\alpha_2)=0$. Ce polynôme d'une variable F s'annulant en α_2, il est forcément un multiple de $C_2(x)=x^2+1$, le polynôme minimal sur $\mathbb{Q}$ de α_2 (car **irréductible** sur $\mathbb{Q}$). Donc $r=q_1C_1+q_2C_2\in\mathfrak{S}$ est une relation symétrique.

Réponse 2. Oui. En utilisant les théorèmes des cours 9 et 10, nous savons que $G_{(\alpha_1,\alpha_2)}$ est le stabilisateur de l'idéal maximal des $\boldsymbol{\alpha}$-relations et que tout idéal maximal est engendré par un ensemble triangulaire séparable $<F_1,F_2>$. Puisque le polynôme non nul $F_2(x_2)$ sur $\mathbb{Q}$ s'annule en α_2, il est nécessairement un multiple de C_2, le **polynôme minimal** de α_2. D'où $F_2\in\mathfrak{S}$. En divisant par C_1 en x_1, le polynôme unitaire de degré 1 en x_1, $F_1(x_1,x_2)$ se réduit à $R(x_2)=F_1(-x_2,x_2)$ qui s'annulant en α_2 est donc un multiple de C_2. D'où $F_1\in\mathfrak{S}$. Ainsi $<F_1,F_2>=\mathfrak{S}$ et $G_{(\alpha_1,\alpha_2)}=S_2$. (si F_1 et F_2 sont unitaires et F_1 est réduit modulo x_2, on montre que $F_i=C_i$).

[1] Soit b le reste de la division euclidienne d'un polynôme $g(x)\in k[x]$ par $ax+b$, $a\neq 0, b\in k$: $g(x)=q(x)\times(ax+b)+\lambda$ avec $\lambda\in k$; d'où, on a bien $\lambda=g(-b/a)$, c-a-d que le reste est la substitution de x par $-b/a$ dans g.

Commentaire. Dans les cours prochains, nous allons présenter des outils généraux qui offriront des réponses simples et directes à toutes ces sortes de questions.

2.3 Que calcule $R:=\mathrm{Res}_{x_2}(C_2(x_2),\mathrm{Res}_{x_1}(C_1(x_1,x_2),x-(x_1-x_2)))$?

Réponse. Rappelons que pour deux polynômes non nuls de $k(x)$ de degré m et $P(x)=a_n(x-u_1)\cdots(x-u_n)$ ainsi scindé dans $\overline{k}[x]$, on a $\mathrm{Res}_x(f,g)=a_n^m\prod_{i=1}^n Q(u_i)$. Puisque $C_1(x_1,x_2)=1\cdot(x_1-(-x_2))$, nous avons $R_1:=\mathrm{Res}_{x_1}(C_1(x_1,x_2),x-(x_1-x_2))=x-(-x_2-x_2)=x-2x_2$ et $R=\mathrm{Res}_{x_2}(C_2,R_1)=(x-2i)(x-2\times(-i))=(x-2i)(x+2i)=x^2+4$. C'est le

polynôme dont les racines sont les $-2\alpha = (-\alpha) - \alpha$ où α est racine de $f = x^2 + 1$; ou plus exactement les racines sont les $\beta - \alpha$ où $\alpha, \beta = -\alpha$ sont les deux racines de f.

2.4 Remplacer $x_1 - x_2$ par $p(x_1, x_2)$. Montrer que $R = \chi_{p,\mathfrak{S}}$, le polynôme caractéristique de l'endomorphisme multiplicatif $\hat{p}$ induit p dans $\mathbb{Q}[x_1, x_2]/\mathfrak{S}$. Soit $\gamma = p(\alpha_1, \alpha_2)$. Constater que $\min_{\gamma,\mathbb{Q}}$ est un facteur de R.

Réponse. On voit comme à la question précédente que $R = (x - p(i,-i))(x - p(-i,i)) = \chi_{p,\mathfrak{S}}$ puisque $\mathfrak{S}$ est radical (les solutions dans $V(\mathfrak{S}) = \{(i,-i),(-i,i)\}$ sont de multiplicité 1). Le polynôme $R \in \mathbb{Q}[x]$ possède γ comme racine. Donc $\min_{\gamma,\mathbb{Q}}$ est un facteur de R.

2.5 Soient $a, b, p \in k[\boldsymbol{x}]$ avec $a \neq 0$ et b de degré 0 en x_1. Remarquez que $\mathrm{Res}_{x_1}(ax_1 + b, y - p(\boldsymbol{x})) = y - p(-b/a, x_2, \ldots x_n)$? Qu'en concluez-vous ?

Réponse. L'identité est évidente. Le résultat est identique au reste de la division en x_1 de $y - p(\boldsymbol{x})$ par $ax_1 + b$ vue en [1] plus haut.

2.6 Pourquoi R est un carré dans $\mathbb{Q}$ avec $p(x_1, x_2) = x_1^2 + x_2^2$? Est-ce le cas chaque fois que p est symétrique en x_1, x_2 ?

Réponse. car $R = \chi_{p,\mathfrak{S}} = (x - p(i,-i))(x - p(-i,i)) = (x - p(i,-i))^2$ car p est symétrique. La symétrie de p nous renseigne a priori.

Commentaire. Nous montrerons que dans le cas général si $p(\boldsymbol{x})$ est un polynôme de n variables de stabilisateur un groupe H dans S_n alors $\chi_{p,\mathfrak{S}} = \mathscr{L}^{\#H}$, où $\mathscr{L}$ est la fameuse **résolvante de Lagrange** qui inspira Galois pour sa non moins fameuse **résolvante de Galois** (une résolvante de Lagrange particulière) et sur laquelle ce dernier fonda sa théorie dite de Galois.

2.7 (Annexe) Que calcule $\mathrm{Res}_{x_2}(f(x_2), \mathrm{Res}_{x_1}(f(x_1), x-(x_1-x_2)))$? Qu'en concluez-vous?

Réponse. $R = \mathrm{Res}_{x_2}(f(x_2), \mathrm{Res}_{x_1}(f(x_1), y - (x_1 - x_2))) = y^2(y^2+4) = \prod_{f(\alpha)=f(\beta)=0}(y - (\alpha - \beta)) = y^2\chi_{x_1-x_2,\mathfrak{S}}$. Pour calculer $\chi_{x_1-x_2,\mathfrak{S}}$, avec les modules de Cauchy, si (α_1, α_2) sont les racines de f, on ne retrouve pas le facteur parasite $y^2 = (y - (\alpha_1 - \alpha_1))(y - (\alpha_2 - \alpha_2)) = \chi_{0,\mathfrak{S}}$.

Commentaire. Cette méthode pour calculer le polynôme $\chi_{p(x_1,x_2),\mathfrak{S}}$ sans les modules de Cauchy fut proposée par Lagrange qui devait ensuite calculer les facteurs parasites, pour les diviser du résultat R. Ici le facteur parasite est

$$\chi_{p(x_2,x_2),\mathfrak{S}} = \mathrm{Res}_{x_2}(f(x_2), y) = y^2$$

(attention, y est une constante). Avec un degré plus élevé de f (i.e. un nombre de variables $x_1,\dots,x_n$ supérieur à 2), chaque nouveau calcul pour retirer un facteur parasite engendre un autre calcul pour retirer les nouveaux facteurs parasites engendrés. Comme le nombre de variables décroit à chaque étape, l'algorithme se termine bien et il est possible de calculer le polynôme caractéristique. Pour calculer un polynôme caractéristique, nous préférerons éviter les facteurs parasites en utilisant les modules de Cauchy.

Exercice 3
Soit $f(x) = x^3+1 = (x+1)(x^2-x+1)$; nous savons que les racines sont $\alpha_1 = -1, \alpha_2 = e^{i\pi/3}, \overline{\alpha_2}$.

3.1 Donner un ensemble triangulaire engendrant l'idéal des relations symétriques de f.

Réponse. Nous calculons les modules de Cauchy : $C_3(x_3) = f_3(x_3) = x_3^3+1$ et sans utiliser de formule directe, $C_2(x_2,x_3) = (x_2^3-x_3^3)/(x_2-x_3) = x_2^2+x_2x_3+x_3^2$ et $C_2(x_1,x_2,x_3) = x_1+x_2+x_3$ (la somme des racines est nulle ...) .

3.2 Soit $\boldsymbol{\alpha} = (\alpha_1 = -1, \alpha_2, \alpha_3)$ un n-uplet des 3 racines de f. Soit la $\boldsymbol{\alpha}$-relation $r = x_2^3 - x_1$. Trouver $\tau \in S_3$ qui n'envoie pas r dans $Id(\boldsymbol{\alpha})$. Le groupe de Galois est-il S_3 ?

Réponse. La permutation $\tau = (1,2)$ envoie r sur $\tau\cdot r = x_1^3 - x_2$. Nous avons $\tau\cdot r(\boldsymbol{\alpha}) = 1-\alpha_2$ qui ne peut être nulle puisque le polynôme minimal de α_2 est $g(x) := x^2-x+1$. Comme τ, n'appartient pas au groupe de Galois $G_{\boldsymbol{\alpha}}$, ce dernier n'est pas le groupe symétrique S_3.

3.3 Donner un ensemble triangulaire engendrant l'idéal maximal $Id(\boldsymbol{\alpha})$. Donnez les éléments du groupe de Galois $G := G_{\boldsymbol{\alpha}}$.

Réponse. 3.3 À partir de la factorisation de f, nous constatons que les polynômes $f_3(x_3) = x_3^2 - x_3 + 1$, $f_2 = x_2 + x_3 - 1$ (la somme $\alpha_3+\alpha_2$ est l'opposé de -1, le coefficient sous-dominant de g) et $f_1(x_1) = x_1 + 1$ sont les $\boldsymbol{\alpha}$-relations et forment un système triangulaire séparable qui engendre l'idéal galoisien I de variété $V = \{(\alpha_1 = 1, \alpha_2 = \frac{1+i\sqrt{3}}{2}, \alpha_3 = \overline{\alpha_2}), (1,\alpha_3,\alpha_2)\}$. On a $V = G \star (1,\alpha_2,\alpha_3)$ où $G = ((1)(2)(3),(2,3))$ est un groupe. D'après l'Identité (3.18) du cours, $V = Inj(I, I_{\boldsymbol{\alpha}}) \star \boldsymbol{\alpha}$; donc G est l'injecteur de I dans $I_{\boldsymbol{\alpha}}$; comme l'injecteur est un groupe, il est donc aussi le stabilisateur de I et par conséquent I est un idéal galoisien pur (voir Theorem 3.50). On peut aussi le vérifier directement sur I : (i) G stabilise I puisque G stabilise f_1 et f_2 ; et pour f_3 : $\tau = (2,3)$ envoie f_3 sur $\tau\cdot f_3 = x_2^2 - x_2 + 1$ qui divisé par f_2 en x_2 donne le reste (voir [1]) : $(-x_3+1)^2 - (-x_3+1) + 1 = x_3^2 - x_3 + 1 = f_3$ d'où $\tau\cdot f_3 \in I$ et (ii) on peut vérifier qu'une permutation de S_3 qui n'appartient pas à G, n'appartient pas non plus à $Inj(I, I_{\boldsymbol{\alpha}})$.

Pour montrer que $I = Id(\boldsymbol{\alpha})$ et que G est bien $G_{\boldsymbol{\alpha}}$, nous pouvons procéder comme pour l'Exercice 2 en prenant une quelconque $\boldsymbol{\alpha}$-relation et en montrant qu'elle se réduit à zéro modulo I. Changeons de méthode. Puisque l'injecteur est un groupe, il contient le groupe de Galois qui ne peut donc être que G ou le groupe identité. Par le théorème de Galois 3.41, tout $\gamma = \Gamma(\boldsymbol{\alpha})$ invariant par $G_{\boldsymbol{\alpha}}$ appartient à $\mathbb{Q}$. Si le groupe de Galois était l'identité, il laisserait invariant x_3 et donc α_3 qui par conséquent appartiendrait à $\mathbb{Q}$; ce qui est faux puisque f_3, son polynôme minimal sur $\mathbb{Q}$, est de degré 2. Donc $G = G_{\boldsymbol{\alpha}}$ et $I = Id(\boldsymbol{\alpha})$.

3.4 Vérifier que $\{(1)(2)(3),(1,2),(1,3)\}$ est une transversale à droite de G mod S_3. Combien d'idéaux co-maximaux contiennent $\mathfrak{S}$? Pouvez-vous les exprimer à partir de $Id(\boldsymbol{\alpha})$? Donner leurs générateurs respectifs.

Réponse. Rappelons que $G\tau \star \boldsymbol{\alpha} = \{\boldsymbol{\alpha}^{g\tau} \mid g \in G\}$. De la décomposition de S_3 en classe à droite modulo G : $S_3 = G + G(1,2) + G(1,3)$, où "+" désigne l'union disjointe, nous déduisons que

$$S_3 \star \boldsymbol{\alpha} = V(\mathfrak{S}) = V(G \star \boldsymbol{\alpha}) \cup V(G(1,2) \star \boldsymbol{\alpha}) \cup V(G(1,3) \star \boldsymbol{\alpha});$$

d'où

$$Id(S_3 \star \boldsymbol{\alpha}) = \mathfrak{S} = Id(G \star \boldsymbol{\alpha}) \cap Id(G(1,2) \star \boldsymbol{\alpha}) \cap Id(G(1,3) \star \boldsymbol{\alpha}).$$

Rappelons que $Inj(Id(L \star \boldsymbol{\alpha}), Id(\boldsymbol{\alpha})) = G_\alpha L \star \boldsymbol{\alpha}$. Et que $Id(L \star \boldsymbol{\alpha}) = Id(G_\alpha L \star \boldsymbol{\alpha})$; ainsi, nous avons

$$\mathfrak{S} = Id((\alpha_1 = 1, \alpha_2, \alpha_3)) \cap Id((\alpha_2, \alpha_1, \alpha_3)) \cap Id((\alpha_3, \alpha_2, \alpha_1)) \quad .$$

Il y a donc bien trois idéaux co-maximaux contenant $\mathfrak{S}$. Rappelons que, d'après le cours, $Gal_{\mathbb{Q}}(\boldsymbol{\alpha}^\sigma) = \sigma^{-1} Gal_{\mathbb{Q}}(\boldsymbol{\alpha})\sigma$ et $Id(\boldsymbol{\alpha}^\sigma) = \sigma^{-1} \cdot Id(\boldsymbol{\alpha})$. Donc, puisque $Id(\boldsymbol{\alpha}) =< f_1(x_1) = x_1 + 1, f_2 = x_2 + x_3 - 1, f_3(x_3) = x_3^2 - x_3 + 1$, nous avons avec $\sigma = (1,2)$

$$Id((\alpha_2, \alpha_1, \alpha_3)) =< f_2(x_1, x_3), f_1(x_2), f_3(x_3) >$$

de stabilisateur $(1,2)^{-1}G(1,2) =< (1,3) >$ (i.e. le groupe de Galois sur $\mathbb{Q}$ de $(\alpha_2, \alpha_1, \alpha_3)$) et avec $\sigma = (1,3)$, nous avons $Id((\alpha_3, \alpha_2, \alpha_1)) =< f_3(x_1) = x_1^2 - x_1 + 1, f_2(x_2, x_1) = x_2 + x_1 - 1, f_1(x_3) = x_3 + 1 >$ de stabilisateur $(1,3)^{-1}G(1,3) =< (1,2) >$. Nous remarquons que l'ensemble triangulaire, si nous voulons le voir comme dans le cours, il faut poser $y_1 = x_2, y_2 = x_1$ et $y_3 = x_3$; ainsi $Id(\alpha_3, \alpha_2, \alpha_1) =< f_2(y_1, y_2) = y_1 + y_2 - 1, f_3(y_2) = y_2^2 - y_1 + 1, f_1(x_3) = x_3 + 1 >$.

Exercice 4

Soit $f \in k[x]$ un polynôme de degré n de racines deux-à-deux distinctes $\alpha_1, \alpha_2, \ldots, \alpha_n$ et $\phi \in k[\boldsymbol{x}]$.

4.1 Soit $r_0 = \phi$ et pour $i = 1, \ldots, n$, soit r_i le reste de la division de r_{i-1} par C_i en x_i. Montrez qu'en divisant ainsi successivement ϕ par les termes de la suite des modules de Cauchy $C_1(x_1, \ldots, x_n), \ldots, C_n(x_n)$, le degré du dernier reste r_n en la variable x_i est strictement inférieur au degré i de C_i en x_i.

Réponse. Considérons $\phi \in k[\boldsymbol{x}]$ et le dernier reste r_n de ses divisions euclidiennes successives par $C_1(x_1), \ldots, C_n(x_n)$ et dans cet ordre. Montrons que pour tout $i \in [\![1, n]\!]$, le degré de r_n en la variable x_i est strictement inférieur au degré $d_i = i$ de C_i en x_i. En effet, il résulte d'un processus de divisions euclidiennes qui commence par la division de ϕ par $C_1(x_1)$ en x_1 avec $\deg_{x_1}(r_1) < \deg_{x_1}(C_1)$. Si, par hypothèse de récurrence, pour $i \in [\![2, n]\!]$, le reste r_{i-1} est en x_j de degré $< \deg_{x_j}(C_j)$ pour tout $j < i$, le reste r_i de la division en x_i de r_{i-1} par $C_i(x_i, \ldots, x_n)$ de degré 0 en $x_1, \ldots, x_{i-1}$ et i en x_i est aussi en x_j de degré $< \deg_{x_j}(C_j)$ pour tout $j < i$ mais aussi en x_i de degré $< \deg_{x_i}(C_i)$ (car division par $C_i(x_i)$ en x_i).

4.2 Soit $r \in k[\boldsymbol{x}]$. Montrer par récurrence que si r satisfait les conditions suivantes :
(i) r est une relation symétrique
(ii) pour tout $j \in [\![1, n]\!]$ $\deg_{x_j}(r) < \deg_{x_j}(C_j) = j$
alors $r = 0$. Vous le montrerez pour $r \in k[x_n]$ puis pour $r \in k[x_j, \ldots, x_n]$, en supposant que c'est vrai sur $k[x_{j+1}, \ldots, x_n]$.

Réponse. D'après le cours, toute relation symétrique s'écrit sous la forme

$$\sum_{i=1}^{n} q_i(\boldsymbol{x}) C_i(x_i, \ldots, x_n) \quad .$$

Supposons que $r \in k[x_n]$. Puisque r est une relation symétrique, $r(x_n) = q(x_n)C_n(x_n)$. Comme r est de degré strictement inférieur à celui de C_n, $r(x_n) = 0$. Supposons par hypothèse de récurrence que si $p \in k[x_{j+1}, \ldots, x_n]$, $j \geq 1$, vérifie les conditions (i) et (ii) du lemme alors $p = 0$ et considérons un polynôme $r \in k[x_j, \ldots, x_n]$ qui vérifie (i) et (ii). Puisque $\deg_{x_j}(r) < \deg_{x_j}(C_j) = j$ et $r \in \mathfrak{S}$, nous pouvons écrire

$$r(x_j, \ldots, x_n) = a_{j-1}(x_{j+1}, \ldots, x_n)x_j^{j-1} + \cdots + a_0(x_{j+1}, \ldots, x_n) = q_j(x_j, \ldots, x_n)C_j(x_j, \ldots, x_n) + q$$

avec $q = \sum_{i=j+1}^{n} q_i C_i \in < C_{j+1}, \ldots, C_n >$; i.e. $q(x_j, \alpha_{j+1}, \ldots, \alpha_n) = 0$ pour tout $\boldsymbol{\alpha} \in V := \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \mid \sigma \in S_n\}$. Ainsi, pour tout $\boldsymbol{\alpha} \in V$,

$$r(x_j, \alpha_{j+1}, \ldots, \alpha_n) = q_j(x_j, \alpha_{j+1}, \ldots, \alpha_n)C_j(x_j, \alpha_{j+1}, \ldots, \alpha_n) \quad .$$

Puisque $\deg_{x_j}(r) < \deg_{x_j}(C_j) = j$, tout $\boldsymbol{\alpha} \in V$, $r(x_j, \alpha_{j+1}, \ldots, \alpha_n) = 0$. Les coefficients $a_{j-1}(x_{j+1}, \ldots, x_n), \ldots, a_0(x_{j+1}, \ldots, x_n)$ de r en x_j s'annulant sur V, ils sont des relations

symétriques et vérifient ainsi chacun la condition (i). Comme r, ces coefficients vérifient la condition (ii). Ces coefficients sont donc tous nuls par l'hypothèse de récurrence car ils appartiennent à $k[x_{j+1},\ldots,x_n]$. Par conséquent $r=0$ et par récurrence 4.2 est démontré.

4.3 Sous les hypothèse de la question 4.1, le polynôme ϕ est une relation symétrique en les racines de f si et seulement si le dernier reste r_n est nul.

Réponse. Un sens est évident puisque $\mathfrak{S} =< C_1,\ldots,C_n >$, d'après le cours. Inversement, supposons que ϕ soit une relation symétrique en ses racines de f. Le reste r_n obtenu à la fin de cette réduction est une relation symétrique car il résulte de la division d'une relation symétrique ϕ par des relations symétriques, les modules de Cauchy. D'après la question (1), le degré du reste ψ en chaque variable x_i est strictement inférieur au degré de C_i en x_i. Puisque ψ satisfait les conditions (i) et (ii) de la question (2), il est nul.

4.4 Pouvez-vous proposer une méthode pour calculer la valeur dans $\mathbb{Q}$ de tout polynôme symétrique s en $\alpha_1,\alpha_2,\ldots,\alpha_n$ à coefficients dans $\mathbb{Q}$? (En remarquant que $s(\boldsymbol{x})-s(\boldsymbol{\alpha})\in\mathfrak{S}$.) Cette méthode est due à A. Cauchy.

Réponse. Le polynôme $r(\boldsymbol{x})=s(\boldsymbol{x})-s(\boldsymbol{\alpha})\in\mathfrak{S}$. En effet, d'après le théorème fondamental des fonctions symétriques $s(\boldsymbol{\alpha})\in\mathbb{Q}$; d'où $r(\boldsymbol{x})\in\mathbb{Q}[\boldsymbol{x}]$; comme s est symétrique, r l'est également et nous avons $\sigma\cdot r(\boldsymbol{\alpha})=r(\boldsymbol{\alpha})=0$ pour tout $\sigma\in S_n$. D'où $r\in\mathfrak{S}$. Puisqu'en réduisant r modulo les module de Cauchy, le résultat est 0, en réduisant de la même manière $s=r+\lambda$, $\lambda=s(\boldsymbol{\alpha})\in\mathbb{Q}$, le résultat est λ.

Commentaire. Par le Théorème fondamental des fonctions symétriques (et aussi celui de Galois), nous savions a priori que $s(\boldsymbol{\alpha})=\lambda\in Q$. Il s'agissait de savoir si pour tout polynôme symétrique $s(\boldsymbol{x})\in\mathbb{Q}[\boldsymbol{x}]$, la valeur $\lambda\in\mathbb{Q}$ de $s(\boldsymbol{\alpha})$ est ou non systématiquement obtenue par la réduction de s modulo $< C_1,C_2,\ldots,C_n >=\mathfrak{S}$. Nous obtenons ainsi une nouvelle **version effective du théorème fondamental des fonctions symétriques** due à A. Cauchy. .

Notons que la question a son importance car nous savons aussi que si un polynôme $p(\boldsymbol{x})\in\mathbb{Q}[\boldsymbol{x}]$ est invariant par le groupe de Galois $G_{\boldsymbol{\alpha}}$, alors $p(\boldsymbol{\alpha})$ appartient toujours à $\mathbb{Q}$ d'après le Théorème de Galois. On se doute qu'il ne suffit pas que $p(\boldsymbol{\alpha})$ appartienne à $\mathbb{Q}$ pour obtenir sa valeur μ dans $\mathbb{Q}$ en le réduisant modulo les modules de Cauchy (sinon la théorie de Galois s'arrêterait là et le cours avec ...).

Ce que nous étudions là sur $\mathfrak{S}$ se généralisera ainsi à tout idéal galoisien I en remplaçant S_n par l'injecteur de I dans un idéal maximal (quelconque) $\mathrm{Id}(\boldsymbol{\alpha})$. En effet :

Soit I un idéal triangulaire de $\mathbb{Q}[\boldsymbol{x}]$ engendré par une ensemble triangulaire séparable $< f_1(x_1,\ldots,x_n),\ldots,f_n(x_n) >$. Alors en divisant successivement $p \in \mathbb{Q}[x_1,\ldots,x_n]$ par f_n en x_n, puis le reste par f_{n-1} en x_{n-1} et ainsi de suite jusqu'à f_1 en x_1, le dernier reste $\overline{p}$ est la **réduction de p modulo** I de telle sorte que $p-\overline{p} \in$ I et $\overline{p}$ est le seul représentant de p dans $\mathbb{Q}[x_1,\ldots,x_n]$/I tel que son degré en x_i soit strictement inférieur à celui de f_i en x_i. En particulier, si $\lambda \in \mathbb{Q}$ et $p-\lambda \in$ I alors λ est la réduction de p modulo I.

Exercice 5

Soit $n = 6$ et le polynôme $f = x^6+2$ irréductible d'après le critère d'Eisenstein (le nombre premier 2 2 divise tous les coefficients sauf celui de x^6 et son carré ne divise pas la constante). Le but cet exercice est de montrer que l'idéal suivant :

$$\mathrm{I} =< f_1 := x_1-x_4-x_6, f_2 := x_2+x_4+x_6, f_3 := x_3+x_4, f_4 := x4^2+x_4x_6+x_6^2, f_5 := x_5+x_6, f_6 := x_6^6+2 >$$

est un idéal galoisien pur de f de groupe de décomposition

$$\mathrm{L} := \mathrm{D}_6 :=< (1,2)(3,4)(5,6), (1,5,3)(2,6,4), (1,3)(2,4) >$$

"le" groupe dihédral d'ordre 12. Nous cherchons un ensemble triangulaire "réduit" ; i.e. $\deg_{x_i} f_r < d_i = \deg_{x_i}(f_i)$ (sinon on divise f_r par f_i en x_i).

Nous supposons que pour toute racine α de f, les polynômes $x+\alpha$ et $x^2+\alpha x+\alpha^2$ sont des facteurs de f sur son corps de rupture $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/f(x)$. Vous pouvez le vérifier en `Maxima` avec la commande `factor(x^6+2,y^6+2)`.

Question 5.1 Pourquoi l'idéal galoisien I est-il pur ? Nous supposons savoir que dans ce cas, I est triangulaire ; ce qui signifie que I est engendré par un ensemble triangulaire séparable $\{f_1(x_1,\ldots,x_6),\ldots,f_6(x_6)\}$ (voir TD 11).

Réponse. Il existe $\boldsymbol{\alpha}$, un n-uplet des racines de f tel que $\mathrm{G}_{\boldsymbol{\alpha}} \subset$ L puisque le groupe de Galois est inclus dans le groupe dihédral. L'idéal $\mathrm{I} = Id(\mathrm{L}\star\boldsymbol{\alpha})$ est défini par un groupe qui contient le groupe G_α. Donc, d'après le cours, l'idéal I est pur ; i.e. $\mathrm{V(I)} = \mathrm{L}\star\boldsymbol{\alpha}$.

Question 5.2 Posons $d_i := \deg_{x_i} f_i$. Nous supposons savoir que $d_i = 1$ pour $i = 1,2,3,5$ et $d_6 = 6$ (voir TD 11). Pourquoi $d_4 = 2$?

Réponse. L'ensemble $\{x_4^{u_4}x_6^{u_6} \mid 0 \le u_4 < d_4 = \deg_{x_4} f_4, \quad 0 \le u_6 < 6 = d_6$ est une k-base de $k[\boldsymbol{x}]$/I. Elle est de cardinal identique à V(I) car I est un idéal radical. Et comme I est galoisien, le cardinal de sa variété est 12, celui de son

injecteur D_6 dans un idéal galoisien maximal quelconque (ici comme I est pur, cet injecteur est aussi le stabilisateur). Donc, nécessairement, $\deg_{x_4} f_4 = 2$.

Question 5.3 Soit $\boldsymbol{\beta} \in V(I)$. On voudrait choisir $f_5 = x_5 + x_6$ qui correspondrait au facteur $x + \beta_6$ sur $\mathbb{Q}(\beta_6)$. Pour que $x_5 + x_6$ appartienne à I, quelle relation choisir alors pour f_3 ?

Réponse. Puisque $f(x) = (x+\alpha)\$$, nous voyons qu'en prenant $\alpha := \beta_6$, nous pouvons avoir une égalité $\beta_i + \beta_6 = 0$ pour $i \neq 6$ (puisque les racines de f sont les β_i ...). Il existe donc nécessairement une relation $x_i + x_6$. Si nous prenons $i = 5$, nous considérons la relation $x_5 + x_6$. Pour qu'elle appartienne à I, cela doit rester cohérent avec le groupe dihédral D_6. Il suffit de le vérifier sur les générateurs. Ceux qui font intervenir 5 ou 6 sont $s = (1,2)(3,4)(5,6)$ et $t = (1,5,3)(2,6,4)$; la permutation t laisse invariant x_5+x_6 et $s\cdot(x_5+x_6) = x_3+x_4$. Ainsi, on peut prendre $f_5 = x_5 + x_6$ et $f_3 = x_3 + x_4$.

Question 5.4 Avec le facteur $x^2 + \alpha x + \alpha^2$, pouvez-vous choisir $f_4 = x_4^2 + x_4x_6 + x_6^2$?

Réponse. Oui puisqu'en prenant $\alpha := \beta_6$, nous aurons $\beta_i^2 + \beta_i\beta_6 + \beta_6^2 = 0$ pour $i \neq 6$ et $i \neq 5$ puisque β_5 est la racine de l'autre facteur $x + \beta_6$. Comme nous cherchons un polynôme de degré 2, nous pouvons prendre $f_4 = x_4^2 + x_4x_6 + x_6^2$; aussi car les 2 autres relations f_1 et f_2 sont de degré 1 en x_1 et x_2 respectivement.

Question 5.5 En vous servant des fonctions symétriques des racines de $F_4 = x_4^2 + \beta_6 x_4 + \beta_6^2$, que serait alors f_2 ? Cela se vérifie-t-il avec les générateurs de D_6 ?

Réponse. La somme des racines $\beta_4 + \beta_2$ de $F_4 = x_4^2 + \beta_6 x_4 + \beta_6^2$ est $-\beta_6$ l'opposé du coefficient de x_4. D'où $\beta_4 + \beta_2 + \beta_6 = 0$. On a alors $f_2 = x_4 + x_2 + x_6$. Vérifions sur les générateurs de D_6. En permutant f_3 ou f_5 de degré 1, nous ne pouvons pas retrouver f_2. En revanche, $f_2 = x_2 + x_4 + x_6$ est invariant par $(1,5,3)(2,6,4)$ et $(1,3)(2,4)$ et en le permutant par $(1,2)(3,4)(5,6)$ on trouve $x_1 + x_3 + x_5$. Nous savons que la dernière relation est une forme réduite de $x_1 + \cdots + x_6 - (\beta_1 + \cdots + \beta_6) = x_1 + \cdots + x_6$ (la somme des racines est nulle). Donc dans $k[\boldsymbol{x}]/I$, nous avons $[x_1 + x_3 + x_5] = -[x_4 + x_2 + x_6] = -[f_2] = 0$. Donc tous les générateurs de D_6, envoient f_2 dans I.

Question 5.6 Nous savons que $x_1 + \cdots + x_6 - (\beta_1 + \cdots + \beta_6) = x_1 + \cdots + x_6 \in I$ pourrait convenir pour f_1. Le polynôme $f_1 = x_1 - x_4 - x_6$ en serait-il une forme "réduite" mod I?

Réponse. $[x_1 + \cdots + x_6 - (\beta_1 + \cdots + \beta_6)] = [x_1 + \cdots + x_6] = x_1 - x_4 - x_6$ puisque $[x_3 + x_4 + x_5 + x_6] = [f_3 + f_5] = 0$ et $[x_2] = -x_4 - x_6$.
Rappelons que 'réduction" consiste à obtenir un représentant dans $k[\boldsymbol{x}]/I$; soit

ici une combinaisons linéaire dans la base monomiale formée des monômes $x_4^u x_6^v$ avec $u<2$ et $v<6$. Cela s'obtient par des divisions euclidiennes successives avec les f_i comme expliqué dans le cours. Pour les f_i de degré $d_i=1$, la division euclidienne est alors une seule substitution, comme ici avec $[x_2]=-x_4-x_6$ puisque $f_2=x_4+x_2+x_6$.

Question 5.7 Comment vérifier que vous avez bien obtenu les générateurs triangulaires réduits de I ? Faites-le.

Réponse. Nous avons construit notre idéal I afin que la variété soit bien formée de n-uplet $\boldsymbol{\beta}$ de racines de f. Nous voulons vérifier que D_6 est le stabilisateur de I. Montrons d'abord que $D_6 \cdot I \subset I$. Il suffit de le vérifier sur les 3 générateurs de D_6 et sur les 6 de I. Pour f_6, c'est évident. Nous l'avons fait pour f_2. Pour f_1 qui est la forme réduite d'un polynôme symétrique, c'est évident aussi. Pour f_5, nous l'avons fait et nous avons obtenu f_3. On le vérifie pour f_3 : (1,2)(3,4)(5,6) laisse invariant f_3 et les deux autres générateurs envoient f_3 sur x_1+x_2 et $x_1+x_2=f_1+x_4+x_6+f_2-(+x_4+x_6)=f_1+f_2\in I$. Reste à vérifier que f_4 permuté par les 3 générateurs de D_6 s'envoie dans I.
$g_1:=(1,2)(3,4)(5,6)\cdot f_4=x_3^2+x_3x_5+x_5^2$; $[g_1]=[f_4]$ car $[x_3]=-[x_4]$ et $[x_5]=-[x_6]$ en réduisant modulo f_5 et f_3.
$g_2:=(1,5,3)(2,6,4)\cdot f_4=x_2^2+x_2x_6+x_6^2\in I$ puisque β_2 représentée par x_2 est l'autre racine de F_2 ; on peut aussi réduire modulo f_2 mais le calcul est inutile car c'est vrai par construction.
et enfin $(1,3)(2,4)\cdot f_4=x_2^2+x_2x_6+x_6^2\in I$.
Donc $D_6\cdot I\subset I$.

On a vu que l'ordre 12 de D_6 est identique au produit $d=d_1\cdots d_6=1\cdot1\cdot1\cdot2\cdot1\cdot6$ des degrés initiaux de l'ensemble triangulaire engendrant I, identique au cardinal de la variété $V(I)=\mathrm{Inj}(I,\mathfrak{M}_\beta)\star\beta$; soit $\beta\in V(I)$; $L:=\mathrm{Inj}(I,\mathfrak{M}_\beta)$ est de cardinal 12 car f est sans racine multiple ; le groupe D_6 est inclus dans L car il stabilise I. Comme D_6 et L sont de même cardinal, ils sont identiques et D_6 est bien le stabilisateur de I. Ce qui confirme au passage que l'idéal galoisien I est pur.

Nous venons de voir que, de façon général, si un groupe H stabilise un idéal galoisien triangulaire et que son cardinal est identique au produit des degrés initiaux de l'ensemble triangulaire engendrant I, alors à la fois H est le stabilisateur de cet idéal et cet idéal est pur. En particulier, pour tout idéal maximal $\mathfrak{M}$ contenant I, nous avons : $H=\mathrm{Stab}(I)=\mathrm{Inj}(I,\mathfrak{M})$.

Exercice 6 Réponse. Cours 12.

Corrigés TD 11 - Annick Valibouze

Corrigé Exercice 1 TD11

Soit le polynôme $f(x) = x^6 + 2$ irréductible sur $\mathbb{Q}$ (voir TD 10). Nous supposons savoir que le groupe de Galois de f est inclus dans "le" groupe dihédral de degré 6 et d'ordre 12. Soit ce groupe dihédral $L := D_6 :=< (1,2)(3,4)(5,6), (1,5,3)(2,6,4), (1,3)(2,4) >$ définissant un idéal galoisien I de f. Un calcul rapide dans le logiciel `SageMath` fournit les informations suivantes : en posant, $L_{(7)} = L = D_6$, nous obtenons :

$$L_{(6)} = L_{(5)} = \{Id, (1,3)(2,4)\} \text{ et } L_{(4)} = L_{(3)} = L_{(2)} = L_{(1)} = \{id\} \quad .$$

Pour décrire l'arbre de la variété, nous utilisons :
$L_{(6)}/L_{(5)} = L_{(4)}/L_{(3)} = L_{(3)}/L_{(2)} = L_{(2)}/L_{(1)} = \{id\}$, $L_{(5)}/L_{(4)} = L_{(5)}$ et

$L_{(7)}/L_{(6)} = \{id, (3,5)(4,6), (1,2)(3,4)(5,6), (1,2)(3,6)(4,5), (1,3,5)(2,4,6), (1,4,5,2,3,6))$

1.1 Pourquoi l'idéal galoisien I est-il engendré par un ensemble triangulaire séparable $\{f_1(x_1,\ldots,x_6),\ldots,f_6(x_6)\}$. Nous supposons cet ensemble réduit.

Réponse. L'idéal I est engendré par un ensemble triangulaire séparable car il est pur (voir Cours).

1.2 A partir des $L_{(i)}$, donnez les formes des polynômes f_i et F_i ?

Réponse. Soit d_r le degré de f_r et de F_r en x_r. Nous avons $d_r = \frac{\#L_{(r+1)}}{\#L_{(r)}}$. Donc $d_6 = 6, d_5 = d_3 = d_2 = d_1 = 1$ et $d_4 = \#(L_{(5)}/L_{(4)}) = 2$. Pour tout $\boldsymbol{\beta} \in V(I)$, nous avons $F_r(x_r) = f_r(x_r,\ldots,\beta_n) = 0$ avec $F_r(\beta_r) = 0$.
$F_6(x_6) = (x_6-\beta_1)(x_6-\beta_2)\cdots(x_6-\boldsymbol{\beta_6})$ puisque l'orbite de 6 par $G = L_{(7)}/L_{(6)}$ est $\{1,2,3,4,5,6\}$ ("orbite de 6 par G" signifie "toutes les permutations de 6 par G"). Aussi, $F_6(x_6) = f_6(x_6) = f(x_6) = x^6 + 2$; nous retrouvons bien $d_6 = 6$.
Puisque $L_{(6)}/L_{(5)} = \{id\}$ et $F_5(\beta_5) = 0$ alors $F_5 = x_5 - \beta_5$; aussi $f_5 = x_5 + g_5(x_6)$ où $\deg_{x_5} g_5 < 6 = d_6$ (sinon on divise par f_6).
On a $L_{(5)}/L_{(4)} = \{Id, (1,3)(2,4)\}$ et $F_4(\beta_4) = 0$; donc $F_4 = (x_4 - \alpha_4)(x_4 - \alpha_2)$ puisque pour avoir les autres racines, nous permutons 4 par $L_{(5)}/L_{(4)}$; aussi $f_4 = x_4^2 + g_4(x_4, x_6)$ avec $\deg_{x_4} g_4 < 2$ et $\deg_{x_6} g_4 < 6$.
De même, avec $L_{(4)}/L_{(3)} = L_{(3)}/L_{(2)} = L_{(2)}/L_{(1)} = \{id\}$, nous avons :
$F_3(x_3) := f_3(x_3, \alpha_4, \alpha_5, \alpha_6) = x_3 - \alpha_3$, $f_3 = x_3 + g_3(x_4, x_6)$
$F_2(x_2) = x_2 - \alpha_2$, $f_2 = x_2 + g_2(x_4, x_6)$
$F_1(x_1) = x - \alpha_1$ et enfin $f_1 = x_1 + g_1(x_4, x_6)$
où pour tout $i \in [[1,4]]$, pour que f_i soit "réduit" il faut que $\deg_{x_4} g_i < 2$ et $\deg_{x_6} g_i < 6$.

Corrigé Exercice 2 TD 11
Nous cherchons à déterminer un idéal maximal et son groupe de décomposition, le groupe de Galois.

2.1 En vous servant de l'expression du polynôme minimal sur $\mathbb{Q}$ (Théorème de Galois), montrez que f est irréductible si et seulement si tout conjugué G de groupe de Galois est transitif ; i.e. pour tout couple i, j dans $[\![1,n]\!]$ il existe $g \in G$ tel que $g(i) = j$. (Devoir)

2.2 Le groupe de Galois de f peut-il être un sous-groupe propre de C_6 ?

Réponse. C_6 possède 6 éléments. Comme le groupe de Galois sur $\mathbb{Q}$ est transitif (f est irréductible sur $\mathbb{Q}$) il faut au moins 6 permutations nécessairement distinctes pour envoyer 1 sur $\{1,2,\ldots,6\}$. Donc, il ne peut être contenu strictement dans C_6.

2.3 En déduire les deux groupes de Galois possibles pour $f = x^6 + 2$.

Réponse. A conjugaison près, n'y a que deux sous-groupes transitifs dans D_6 : D_6 et C_6 (ou son conjugué $\sigma C_6 \sigma^{-1}$, $\sigma = (3,5)(4,6)$).

2.4 Quel est le degré de la résolvante $R_{P,I}$? Quelles sont ses racines (formellement).

Réponse. Comme $\mathrm{Stab}_{D_6}(P) = C_6$, le degré de la résolvante $R_{P,I}$ est $2 = \#D_6/\#C_6 = [C_6 : D_6]$, l'indice de C_6 dans D_6 ; cela se voit sur l'union disjointe de classes à gauche : $D_6 = C_6 + \sigma C_6$ puisque $C_6 \cdot P = P$ et $\sigma C_6 \cdot P = \sigma \cdot P$; d'où $D_6 \cdot P = \{P, \sigma \cdot P\}$. Ainsi

$$R := R_{P,I} = \prod_{Q \in D_6 \cdot P} (x - Q(\boldsymbol{\alpha})) = (x - P(\boldsymbol{\alpha}))(x - \sigma \cdot P(\boldsymbol{\alpha})) \quad .$$

2.5 Calculer les réductions modulo I des éléments de l'orbite $D_6 \cdot P$. Qu'en concluez-vous ?

Réponse. Pour calculer ce polynôme R, nous allons calculer la somme et le produit de ses racines : par exemple, pour la somme, $S = [P + \sigma \cdot P] = [[P] + [\sigma \cdot P]]$ (on réduit d'abord les polynômes modulo I avant de faire les calculs avant de les simplifier). Cette réduction a été vue plusieurs fois : il s'agit de faire des divisions euclidiennes. Ici nous avons :
$[P] = [x_5 x_4^2 + x_6 x_3^2 + x_2 x_5^2 + x_3 x_2^2 + x_1 x_6^2 + x_4 x_1^2]$; puisque $[x_5] = -[x_6]$ (on peut aussi écrire $\alpha_5 = -\alpha_6$) et $[x_3^2] = [x_4^2]$ (i.e. $\alpha_3^2 = \alpha_4^2$), il vient $[x_5 x_4^2 + x_6 x_3^2] = [0]$; de même, comme $[x_1] = [x_4 + x_6] = -[x_2]$, il vient $[x_2 x_5^2 + x_1 x_6^2] = [x_2 x_5^2 - x_2 x_6^2] = [0]$; et enfin, $[x_3 x_2^2 + x_4 x_1^2] = [-x_4 x_2^2 + x_4 x_2^2] = [0]$. D'où $[P] = [0]$. Un calcul similaire montre que $[\sigma \cdot P] = [0]$. Nous avons donc $R_{P,I} = x^2$.

Nous ne pouvons rien en conclure sur G_α si ce n'est que P et $\sigma \cdot P$ sont des $\boldsymbol{\alpha}$-relations car ils s'annulent en $\boldsymbol{\alpha}$.

En effet, d'après le cours, si une racine de R appartient à $\mathbb{Q}$ et est **simple**, alors $G_{\boldsymbol{\alpha}} \subset C_6$ pour un certain $\boldsymbol{\alpha} \in V(I)$. Si la racine n'est pas simple, ce n'est plus certain.

2.6 Soit $g(y) \in \mathbb{Q}[y]$, un polynôme non constant et $\Theta = P(g(x_1), \ldots, g(x_6))$. Nous avons $\mathrm{Stab}_{D_6}(P) = C_6$. Nous cherchons g tel que $\Theta(\boldsymbol{\alpha})$ soit une racine simple de $R_{\Theta,I}$. Pourquoi ?

Réponse. D'après le même Théorème du cours, si $G_{\boldsymbol{\alpha}} \subset C_6$ pour un certain $\boldsymbol{\alpha} \in V(I)$ alors R possède une racine dans $\mathbb{Q}$. En d'autres termes, par contraposée, si aucune racine de R n'appartient à $\mathbb{Q}$ alors pour tout $\boldsymbol{\alpha} \in V(I)$, $G_{\boldsymbol{\alpha}} \not\subset C_6$.

Or ici, notre polynôme R est de degré 2. Donc si une racines a n'est pas simple, $R = (x-a)^2$, d'où $a \in \mathbb{Q}$; par conséquent, aucun sens du théorème 5 ne sera utilisable si une racine n'est pas simple.

2.7 Soit $g = x^2$. Notons Θ' l'autre élément de l'orbite de Θ. Avec les mêmes calculs qu'en 2.4, nous trouvons que $[\Theta] = 6x_4x_6^5 + 6$ et $[\Theta'] = -6x_4x_6^5 + 18$. Soit $r := \Theta - \Theta'$. En vous servant des générateurs de I, montrer que $r(\boldsymbol{\alpha}) \neq 0$.

Réponse. $[\Theta] = 6x_4x_6^5 + 6$ et $[\Theta'] = -6x_4x_6^5 + 18$. On veut savoir si $\Theta(\boldsymbol{\alpha}) = \Theta'(\boldsymbol{\alpha})$; i.e si le polynôme $r := \Theta - \Theta'$ est ou non une $\boldsymbol{\alpha}$-relation ? Si le groupe de Galois n'est pas D_6, on peut avoir une relation dans un idéal maximal qui n'appartient pas à I ; en particulier, nous pourrions avoir $r(\boldsymbol{\alpha}) = 0$ (i.e. la classe de r modulo l'idéal maximal est nulle) alors que $[r] \neq [0]$ (i.e. modulo I). Regardons tout de même s'il se peut que $r(\boldsymbol{\alpha}) = 0$: $r(\boldsymbol{\alpha}) = 12\alpha_4\alpha_6^5 - 12 = 0$ ssi $\alpha_4\alpha_6^5 = 1$; soit $\alpha_4\alpha_6^6 = \alpha_6$; d'où $2\alpha_4 = -\alpha_6$ puisque $\alpha_6 \neq 0$,. Comme $\alpha_2 + \alpha_4 + \alpha_6 = 0$, on trouve $\alpha_2 = \alpha_4$; ce qui est impossible puisque les racines de f sont 2-à-2 distinctes. Donc $r(\boldsymbol{\alpha}) \neq 0$ et nous n'avons pas eu besoin de calculer la résolvante pour savoir si le discriminant de la résolvante est nul ou non.

Par conséquent, sans aller plus loin dans le calcul de R, nous savons que ses racines sont distinctes.

2.8 Calculer $R_{\Theta,I}$. Qu'en concluez-vous ?

Réponse. Pour la somme des racines : $S = [[\Theta] + [\Theta']] = 24$ (sans calcul) et pour le produit des racines : $P = [[\Theta]\cdot[\Theta']] = 36[(x_4x_6^5+1)(-x_4x_6^5+3)]$; en divisant P par f_4 en x_4 puis f_6 (divisions euclidiennes) , nous trouvons 252. D'où $R_{\Theta,I}$ est le polynôme $x^2 - 24x + 252$ irréductible sur $\mathbb{Q}$. D'après le cours, nous en concluons que, pour tout $\boldsymbol{\alpha} \in V(I)$, $D_6 = G_{\boldsymbol{\alpha}}$ et $I = \mathrm{Id}(\boldsymbol{\alpha})$ l'idéal maximal $\mathfrak{M}_{\boldsymbol{\alpha}}$.

Corrigé TD 12 - Annick Valibouze

Rappels de cours : Lorsque f est irréductible sur $\mathbb{Q}$, pour tout n-uplet $\boldsymbol{\alpha}$ de ses racines, le groupe de permutations $G_{\boldsymbol{\alpha}}$, dit de Galois, est transitif.

L'idéal galoisien I est dit pur si son stabilisateur s'identifie à chacun de ses injecteurs dans un idéal maximal qui le contient (il faut et il suffit qu'il s'identifie à un seul de ces injecteur pour qu'il s'identifie à tous). Si I est pur alors il est triangulaire et $V(I) = \mathrm{Stab}(I) \star \boldsymbol{\alpha}$ pour tout $\boldsymbol{\alpha} \in V(I)$. Tout idéal triangulaire n'est pas nécessairement pur.

Soit $\mathfrak{M}$ un idéal maximal contenant I. Si le stabilisateur de $\mathfrak{M}$ (i.e. un groupe de Galois) est inclus dans le stabilisateur de I alors I est pur. En particulier, pour $I := I_{\boldsymbol{\alpha}}^{H}$, où H est un groupe, si $G_{\boldsymbol{\alpha}} \subset H$ alors I est pur car H est nécessairement un sous-groupe de Stab(I) et on peut prendre $\mathfrak{M} = \mathrm{Id}(\boldsymbol{\alpha})$.

Pour qu'un idéal I soit galoisien, il faut et il suffit que I soit radical et que $V(I) \subset V(\mathfrak{S})$. En effet, dans ce cas $I = \mathrm{Id}(V(I))$ et $V(I) = L \star \boldsymbol{\alpha} \subset S_n \star \boldsymbol{\alpha}$ où $L \subset S_n$; donc $I = \mathrm{Id}(L \star \boldsymbol{\alpha})$ qui est bien galoisien.

Corrigé Exercice 1 TD 12

Soit $f \in \mathbb{Q}[x]$ et I un idéal galoisien de f.

1.1 La résolvante $R_{P,\mathfrak{S}} = (x-1)x^8(x^2-8)^5(x^4-8x^2+14)^4$ possède une racine simple dans $\mathbb{Q}$. Qu'en concluez-vous ?

Réponse. Comme la résolvante $R_{P,\mathfrak{S}}$ possède un facteur linéaire et simple sur $\mathbb{Q}$, il existe $\boldsymbol{\alpha} \in V(\mathfrak{S})$ tel que $G_{\boldsymbol{\alpha}} \subset M$ et donc l'idéal galoisien $I := I_{\boldsymbol{\alpha}}^{M}$ est pur ; de plus, le facteur linéaire étant $x-1$ alors, d'après le théorème de l'élément primitif, :

$$I = \mathfrak{S} + < P - 1 >$$

avec $V(I) = M \star \boldsymbol{\alpha}$; d'où $\mathrm{Card}(V(I)) = 1152$, l'ordre de M, le stabilisateur de I.

1.2 Soit $I = I_{\boldsymbol{\alpha}}^{M}$ l'idéal galoisien du 1. Nous trouvons 3 idéaux triangulaires J_1, J_2, J_3 tels que pour chacun le produit des degrés initiaux est 384 et $I = J_1 \cap J_2 \cap J_3$. Qu'en concluez-vous ?

Réponse. Fixons $i \in \{1,2,3\}$ et $\boldsymbol{\alpha} \in V(I)$. Nous avons $V(I) = V(J_1) \cup V(J_2) \cup V(J_3)$, avec $\mathrm{Card}(V(J_i)) \leq 384 = \dim \mathbb{Q}[\boldsymbol{x}]/J_i$, le produit des degrés initiaux de J_i. On ne sait pas encore que J_i est radical, on va le montrer. Comme $\mathrm{Card}(V(I)) \leq \mathrm{Card}(V(J_1)) + \mathrm{Card}(V(J_2)) + \mathrm{Card}(V(J_3)) \leq 3 \cdot 384 = 1152 = \mathrm{Card}(V(I))$, on a nécessairement $\mathrm{Card}(V(J_i)) = 384$ avec $V(J_i) \cap V(I_j) = \emptyset$ pour tout $j \neq i$. Puisque $\mathrm{Card}(V(J_i)) = 384 = \dim \mathbb{Q}[\boldsymbol{x}]/J_i$, l'idéal J_i est radical. Comme, de plus, $V(J_i) \subset V(I)$, l'idéal J_i est galoisien. Soit $M_i = \mathrm{Inj}(J_i, \mathrm{Id}(\boldsymbol{\alpha}))$,

ensemble de permutations de cardinal 384. Nous avons $M_i \subset M$, $V(J_i) = M_i \star \boldsymbol{\alpha}$ et $M = M_1 + M_2 + M_3$ (union disjointe d'ensembles de permutations).

1.3 Par la méthode des résultants combien des 8 résultants pourriez-vous éviter pour calculer R_{Θ,J_1} ? Quel est le degré du polynôme que vous obtenez à la fin du calcul ?

Réponse. Soit $u(x) = x + b, v(x) \in \mathbb{Q}[x]$, $b \in \mathbb{Q}$. Alors $\mathrm{Res}_x(u(x), v(x)) = v(-b)$ et le calcul du résultant est superflu. Dans les générateurs triangulaires de J_1, nous avons $x_4 + x_3$ et $x_8 + x_7 + x_6 + x_5$. En particulier, avec $x = x_8$ et $b = x_7 + x_6 + x_5$, nous avons :

$$\mathrm{Res}_{x_8}(x_8 + x_7 + x_6 + x_5, y - \Theta(x_1, \ldots, x_8)) = y - \Theta(x_1, \ldots, x_7, -(x_7 + x_6 + x_5)) \quad .$$

Avec la méthode des résultants, nous calculons le polynôme caractéristique χ_{Θ,J_1}, de degré est 384, le cardinal de la variété puisque l'idéal J_1 est radical.

1.4 Les calculs fournissent ci-dessous les polynômes minimaux des 3 endomorphismes induits par Θ (i.e. les formes sans facteur carré des polynômes caractéristiques). En déduire la résolvante $R_{\Theta,I}$. Qu'en concluez-vous ?

$$\begin{aligned} M_{\Theta,J_1} &= x(x^4 - 4x^2 + 32) \quad \text{et} \\ M_{\Theta,J_2} &= M_{\Theta,J_3} = (x^4 - 4x^2 + 32)(x^4 - 8x^2 - 112) \end{aligned}$$

Réponse. Puisque $V(I)$ est l'union disjointe $V(J_1) \cup V(J_2) \cup V(J_3)$ et que tous les idéaux sont radicaux, par définition du polynôme caractéristique :

$$\chi_{\Theta,I} = \chi_{\Theta,J_1} \cdot \chi_{\Theta,J_2} \cdot \chi_{\Theta,J_3} = x(x^4 - 4x^2 + 32)^3 (x^4 - 8x^2 - 112)^2 \quad .$$

Nous savons que, dans notre contexte, le polynômes minimal de l'endomorphisme multiplicatif $\hat{\Theta}$ est la forme sans facteur carré du polynôme caractéristique. D'où

$$M_{\Theta,I} = x(x^4 - 4x^2 + 32)(x^4 - 8x^2 - 112) \quad .$$

Le polynôme minimal $M_{\Theta,I}$ est aussi la forme sans facteur carré de la résolvante $R_{\Theta,I}$. Le degré de $R_{\Theta,I}$ est l'indice 9 dans M de H, le stabilisateur de Θ dans M car M est le stabilisateur de l'idéal galoisien pur I. Comme les deux polynômes $M_{\Theta,I}$ et $R_{\Theta,I}$ sont de même degré, ils sont identiques. Donc x est un facteur linéaire simple sur $\mathbb{Q}$ de la résolvante. Comme en (1), nous en déduisons qu'il existe $\boldsymbol{\alpha} \in V(I)$ tel que $G_{\boldsymbol{\alpha}} \subset H$; donc l'idéal galoisien $I^H_{\boldsymbol{\alpha}}$ est pur ; de plus, d'après le théorème de l'élément primitif, :

$$I^H_{\boldsymbol{\alpha}} = I + < \Theta >$$

avec $V(I^H_{\boldsymbol{\alpha}}) = H \star \boldsymbol{\alpha}$ et $\mathrm{Card}(V(I^H_{\boldsymbol{\alpha}})) = 128$, l'ordre de H, le stabilisateur de $I^H_{\boldsymbol{\alpha}}$.

1.5 En utilisant la permutation $\tau := (1,5)(2,6)(3,7)(4,8)$ de H, retrouvez cet ensemble triangulaire engendrant $J := I^H_{\boldsymbol{\alpha}}$

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

Réponse. Montrons que $J_1 \subset I_{\boldsymbol{\alpha}}^H$. Il suffit de prouver que $H \subset \mathrm{Inj}(J_1, \mathrm{Id}(\boldsymbol{\alpha})) = M_1$. Supposons par l'absurde que $h \in H$ et $h \notin M_1$. Donc $h \in M_2 \cup M_3$ car $H \subset M = M_1 + M_2 + M_3$. Dans ce cas $h \cdot \Theta(\boldsymbol{\alpha})$ devrait être une racine $M_{\Theta,J_2} \cdot M_{\Theta,J_3}$. Puisque $H = \mathrm{Stab}_M(\Theta)$ et $\Theta(\boldsymbol{\alpha}) = 0$, $x = x - h \cdot \Theta(\boldsymbol{\alpha})$ devrait être un facteur de $M_{\Theta,J_2} \cdot M_{\Theta,J_3}$, ce qui est faux. Donc $J_1 \subset I_{\boldsymbol{\alpha}}^H$ et, en particulier, $r = x_2 + x_1 \in J_1 \subset I_{\boldsymbol{\alpha}}^H$.

Comme H est le stabilisateur de $I_{\boldsymbol{\alpha}}^H$, et $\tau \in H$, nous avons $r_6 = \tau \cdot r = x_6 + x_5 \in I_{\boldsymbol{\alpha}}^H$.

Posons $J :=< T_H >$. Remarquons que $J_1 \subset J$ puisque $x_6^3 + x_6^2 x_5 + x_6 x_5^2 + x_5^3 = r_6(x_6^2 + x_5^2) \in J_1 \cap J$ et que les autres générateurs de J_1 appartiennent à T_H. Montrons que $J = I_{\boldsymbol{\alpha}}^H$. Nous avons, par construction, $J \subset I_{\boldsymbol{\alpha}}^H$. Puisqu'à la fois $V(J) \supset V(I_{\boldsymbol{\alpha}}^H)$ de cardinal 128 et $\mathrm{Card}(V(J)) \leq 128$, le produit des degrés initiaux de l'ensemble triangulaire T_H, il vient $\mathrm{Card}(V(J)) = 128 = \dim \mathbb{Q}[\boldsymbol{x}]/J$. Donc $J = I_{\boldsymbol{\alpha}}^H$ puisque ces deux idéaux sont radicaux (et même galoisiens) et de variétés identiques. (Nous aurions pu aussi affirmer que J est radical car d'après un théorème du cours lorsqu'un idéal est engendré par un ensemble à la fois triangulaire alors il est radical.)

1.6 La réduction de Ψ modulo J est $\Psi' = 128x_1^3 x_3 x_5^3 x_7 + 352$. En calculant $R_{\Psi,J} = R_{\Psi',J}$, nous trouvons $(x-96)(x+608)$. Qu'en concluez-vous ? Pouvez-vous en déduire $I_{\boldsymbol{\alpha}}^G$?

Réponse. Toujours comme en (1), puisque $x - 96$ est un facteur à la fois linéaire et simple, il existe $\boldsymbol{\alpha} \in V(J)$ tel que $G_{\boldsymbol{\alpha}} \subset G$; donc l'idéal galoisien $I_{\boldsymbol{\alpha}}^G$ est pur et, d'après le théorème de l'élément primitif, nous avons :

$$I_{\boldsymbol{\alpha}}^G = J + < \Psi' - 96 >$$

avec $V(I_{\boldsymbol{\alpha}}^G) = G \star \boldsymbol{\alpha}$, $\mathrm{Card}(V(I_{\boldsymbol{\alpha}}^G)) = 64$, l'ordre de G, le stabilisateur de $I_{\boldsymbol{\alpha}}^G$. Notons que si nous choisissons l'autre facteur $x + 608$, le stabilisateur de l'idéal galoisien obtenu est aussi le groupe G.

1.7 Le discriminant de f est $2^{19}7^4$. Qu'en concluez-vous ?

Réponse. Le groupe de Galois $G_{\boldsymbol{\alpha}}$ n'est pas un groupe pair puisque le discriminant de f n'est pas un carré (voir cours).

Pour conclure, en calculant une résolvante par un invariant de la seule classe de conjugaison dans G qui pourrait être celle du groupe de Galois (pourquoi à votre avis ?), nous ne trouvons aucune racine dans $\mathbb{Q}$. Donc le groupe de Galois est bien G. Le calcul avec des techniques qui dépassent le cadre de ce cours aboutissent à l'ensemble triangulaire suivant qui engendre un idéal maximal $I_{\boldsymbol{\alpha}}^G$:

$$T_H \cup \{2x_7 + x_5 x_3 x_1^7 + x_5 x_3 x_1^3\} \setminus \{x_7^2 + x_5^2\}$$

Ces techniques peuvent faire appel à la factorisation dans les extensions (voir (voir Exercice 5 TD10) ou à d'autres comme celles dites des bases de Gröbner.