Enseign. Math. (2) (Online first)
DOI 10.4171/LEM/1082

Published by EMS Press

Sur les équations du 3-ème et du 4-ème degré : de Galois et Lagrange au miracle de Morley

Alain Connes and Jacques Dixmier

Résumé. Le Théorème de Morley en géométrie plane, associe à un triangle 18 triangles équilatères, construits à partir des intersections des trissectrices des angles. Nous généralisons ce théorème en un résultat sur les équations algébriques du troisième et du quatrième degré sur un corps K. Nous associons à un choix cohérent, parmi les 18 possibles, de racines cubiques des birapports des racines, une configuration *équiharmonique* de quatre éléments de la clôture algébrique de K.

Mathematics Subject Classification (2020). Primary 11R16; Secondary 51M04.

Keywords. Equation du 3-è degré, équation du 4-è degré, théorème de Morley, Lagrange, Galois.

L'espoir de trouver du nouveau sur les équations du troisième et du quatrième degré évoque irrésistiblement des chercheurs d'or des siècles passés égarés aujourd'hui à la quête de précieuses pépites dans les rues de San Francisco. Anachronisme sans doute, tant l'article de Lagrange de 1770 [4] semble mettre un point d'orgue à ce sujet.

Notre présentation, qui peut être considérée comme une initiation à la théorie de Galois dans ces cas simples, consiste à donner explicitement les transformations des racines qui proviennent, pour le degré trois de l'action transitive du sous-groupe distingué $A_3 \subset S_3$ et pour le degré quatre du sous-groupe distingué d'ordre 4, $M_4 \subset A_4 \subset S_4$. Cela révèle un lien étroit entre les formules obtenues et les invariants des formes binaires.

Tout cela prépare notre résultat principal qui est une généralisation, dans le cadre des équations du 3-ème et du 4-ème degré, du Théorème de Morley sur les 18 triangles équilatères associés à un triangle. Cette généralisation (Théorème 4.9) associe à un choix cohérent, parmi les 18 possibles, de racines cubiques des birapports des racines, une configuration *équiharmonique*. Il est obtenu en utilisant la preuve algébrique [2] du théorème de Morley.

1. Introduction

Dans tout cet article k désigne un corps commutatif de caractéristique nulle, $\overline{k}$ une clôture algébrique de k et K, $k \subset K \subset \overline{k}$ une extension finie de k. Étant donnés trois éléments distincts $a, b, c \in K$, il existe une transformation affine $g \in A(K)$ unique telle que $g(b) = 1, g(c) = 0$. Elle transforme (a, b, c) en $(\omega, 1, 0)$ où $\omega = \frac{a-c}{b-c}$. Aux six permutations de (a, b, c) correspondent les éléments de l'orbite de ω,

$$\left\{\omega, 1-\omega, \frac{1}{\omega}, \frac{\omega-1}{\omega}, \frac{1}{1-\omega}, \frac{\omega}{\omega-1}\right\}$$

sous l'action du groupe symétrique S_3 sur l'espace projectif $\mathbb{P}^1(K)$. Les orbites de S_3 dans $\mathbb{P}^1(K)$ sont de cardinal 6, sauf les orbites

$$\left\{-1, \frac{1}{2}, 2\right\}, \quad \{0, 1, \infty\}, \quad \{-j, -j^2\},$$

où $1 + j + j^2 = 0$. Si la fonction $V(a, b, c) = \frac{a-c}{b-c}$ prend six valeurs différentes quand on permute (a, b, c) il existe une transformation affine g, uniquement déterminée par le sous-ensemble $\{a, b, c\} \subset K$, et telle que l'on ait

$$g(a) + g(b) + g(c) = 0, \quad \frac{1}{3}\left(g(a)^{-1} + g(b)^{-1} + g(c)^{-1}\right) = 1. \tag{1}$$

Nous commencerons par donner, dans la Section 2, Théorème 2.1, les fractions rationnelles $R_j(\omega)$, qui expriment $g(a), g(b), g(c)$ en fonction de ω, et que l'on obtient en appliquant la méthode de Lagrange (que nous rappelons brièvement au début de la section). Nous montrons dans cette Section 2 comment marche la théorie de Galois pour l'équation du troisième degré quand on utilise la fonction $V(a, b, c)$ pour briser la symétrie entre les racines et que l'on suit sa méthode. C'est l'adjonction d'une racine carrée du discriminant Δ qui réduit le groupe de Galois au groupe alterné A_3 et nous donnons explicitement l'action de celui-ci sur les racines α, β, γ de l'équation $X^3 + pX + q = 0$ par la formule

$$\beta, \gamma = -\frac{\alpha}{2} \pm \frac{-4p^2 + 9q\,\alpha - 6p\alpha^2}{2\sqrt{\Delta}}. \tag{2}$$

Pour l'équation du quatrième degré nous avons obtenu un analogue de la formule (2) qui permet de passer d'une racine à une autre. Le groupe symétrique S_4 a ceci de particulier que le sous-groupe alterné $A_4 \subset S_4$ n'est pas un groupe simple. Il contient un sous-groupe distingué M_4 d'ordre 4, familèrement appelé le "groupe du matelas". C'est l'action transitive de ce sous-groupe sur les racines $(\alpha, \beta, \gamma, \delta)$ de l'équation

$$P(X) = X^4 + pX^2 + qX + r = 0$$

que nous calculons. Le Corollaire 2.2 du Théorème 2.1 donne la solution. Ce corollaire montre que si les six birapports de quatre éléments $(\alpha, \beta, \gamma, \delta)$ d'un corps K sont distincts, il existe une unique transformation projective h de $\mathbb{P}^1(K)$ telle que $h(\alpha) = \infty$ et que $(h(\beta), h(\gamma), h(\delta))$ vérifient les conditions (1). Il donne de plus les fractions rationnelles $R_i(\omega)$ pour $(h(\beta), h(\gamma), h(\delta))$ en fonction du birapport ω de $(\alpha, \beta, \gamma, \delta)$. Or on vérifie que, α étant fixé, et en posant $\rho = P'(\alpha) = 4\alpha^3 + 2\alpha p + q, \sigma = \frac{1}{2}P''(\alpha) = 6\alpha^2 + p$, la transformation projective

$$x \mapsto \frac{1}{x-\alpha} + \frac{\sigma}{3\rho}$$

a les propriétés requises pour h à une homothétie près. En comparant les formules obtenues pour $(h(\beta), h(\gamma), h(\delta))$ on obtient les transformations suivantes de α vers les trois autres racines

$$T_j(\alpha) := \alpha - P'(\alpha)\Big(\frac{p}{3} + 12\frac{J}{I}R_j(\omega) + 2\alpha^2\Big)^{-1} \tag{3}$$

où I et J sont des fonctions polynomiales explicites de p, q, r dont nous donnons l'interprétation géométrique connue en termes des invariants des formes binaires de degré quatre (voir Section 3.1). En fait nous montrons comment arriver directement aux formules (3) donnant l'action de M_4 en utilisant un Lemme 3.1 classique qui donne les résolvantes $\alpha\beta + \gamma\delta, \alpha\gamma + \beta\delta, \alpha\delta + \beta\gamma$ en fonction du birapport ω.

Nous traitons en détail dans la Section 3.3 le cas particulier harmonique : quand les birapports des racines forment l'orbite $\{-1, \frac{1}{2}, 2\}$. Nous donnons les formules pour l'action du groupe de Galois de l'extension galoisienne $K = k(\alpha, \beta, \gamma, \delta)$ dans les trois cas possibles et montrons (Théorème 3.5) que si K est de degré 2 sur le corps $k(\sqrt{\Delta})$ le groupe de Galois de K sur k est $\mathbb{Z}/4$.

Dans la Section 4.1, nous donnons l'interprétation géométrique, dans le cas du corps des complexes, d'une résolvante qui apparaît dans l'article [4] de Lagrange de 1770. Cette interprétation est en termes de l'intersection de quatre cercles circonscrits à des triangles dont deux sommets sont des racines et le troisième une intersection de diagonales du quadrilatère dont les sommets sont les racines.

Enfin nous terminons cet article par une généralisation du théorème découvert par Frank Morley en 1898, qui affirme que les intersections des trissectrices des angles d'un triangle forment un triangle équilatéral. Notre généralisation (Théorème 4.9) s'énonce dans le cadre ci-dessus des équations algébriques de degré 3 et 4. On suppose que K possède une racine cubique $j \in K$, $j \neq 1$, de l'unité, et un automorphisme σ de K sur k tel que $\sigma(j) = j^2, \sigma^2 = \mathrm{Id}$. Nous introduisons (Définition 4.8) la notion de "racine cubique des birapports" de quatre éléments $(\alpha, \beta, \gamma, \delta)$ de K. Cette extraction de racine cubique admet en général 18 solutions. Elles correspondent aux 18 triangles de Morley. Nous construisons une configuration équiharmonique avec les points fixes de produits de deux transformations projectives fixant deux racines et de valeur propre (plus précisement rapport de valeurs propres) donnée par les rapports $u/\sigma(u)$ des racines cubiques u des birapports.

2. L'équation du troisième degré

Le point de départ des travaux d'Abel et de Galois sur la théorie des équations est un lemme, implicite chez Lagrange, et que Galois énonce sous la forme suivante [1] :

(1) Etant donnée une équation quelconque, qui n'a pas de racines égales, dont les racines sont $a, b, c, \ldots$, on peut toujours former une fonction V des racines, telle qu'aucune des valeurs que l'on obtient en permutant dans cette fonction les racines de toutes manières ne soient égales.

(2) La fonction V étant choisie comme il est indiqué dans l'article précédent, elle jouira de cette propriété que toutes les racines de l'équation proposée s'exprimeront rationnellement en fonction de V.

L'équation en V, i.e., $Q(V) = 0$ où le polynôme Q,

$$Q(X) = \prod_{\sigma} \big(X - V(\sigma(a), \sigma(b), \ldots, \sigma(z))\big)$$

s'exprime en fonction des coefficients de l'équation proposée, a la propriété particulière suivante : si x est l'une quelconque de ses racines, toute autre racine s'écrit $R(x)$ où R est une fonction rationnelle à coefficients dans le corps k des coefficients de l'équation. En particulier il suffit d'adjoindre formellement une racine de cette équation, en travaillant avec l'algèbre des polynômes modulo les multiples de Q, pour adjoindre en fait toutes les racines. En général Q n'est pas irréductible et Galois note que, de même, les racines de l'équation $Q_1(V) = 0$ obtenue à partir d'un facteur irréductible de l'équation en V, sont fonctions rationnelles de l'une quelconque d'entre elles et que (en travaillant modulo Q_1) ces fonctions forment un groupe pour la composition. Ce qui est loin d'être évident à ce stade est que ce groupe est en fait indépendant des choix effectués, en particulier celui de la fonction auxiliaire $V(a, b, \ldots)$ et ne dépend donc que de l'équation proposée. Cette indépendance est un point crucial de la théorie de Galois.

Pour l'équation du troisième degré, Lagrange utilise la résolvante

$$V(a, b, c) = a + jb + j^2 c$$

où j est racine cubique de l'unité et montre que l'équation de degré 6 ayant pour racines les 6 valeurs de V obtenues en permutant dans cette fonction les racines de toutes manières, ne fait intervenir que X^3 et X^6 et donc se ramène au degré 2. Comme on le sait il est indispensable d'utiliser les nombres complexes pour résoudre par radicaux une équation de degré 3 dont les trois racines sont réelles, et ce cas là est en effet à l'origine de l'utilisation des nombres complexes.

Soit

$$\Omega := \frac{4}{27}\frac{(1-\omega+\omega^2)^3}{\omega^2(1-\omega)^2}. \tag{4}$$

Alors Ω est un invariant de l'orbite de l'action de S_3

$$\left\{\omega, 1-\omega, \frac{1}{\omega}, \frac{\omega-1}{\omega}, \frac{1}{1-\omega}, \frac{\omega}{\omega-1}\right\}. \tag{5}$$

Etant donnée une équation du 3-ème degré, irréductible à coefficients dans k, dont les racines ne forment pas les sommets d'un triangle équilatère, on peut, par une transformation affine à coefficients dans k, mettre l'équation sous la forme

$$X^3 - 3sX + s = 0. \tag{6}$$

On a en effet $p \neq 0$ une fois l'équation mise sous la forme $x^3 + px + q = 0$ et il suffit de multiplier les racines par $-\frac{1}{3}\frac{p}{q} \neq 0$ pour que le barycentre de leurs inverses soit égal à 1, i.e., que l'équation soit de la forme indiquée.

Quels que soient les éléments $\alpha, \beta, \gamma, \delta \in K \cup \{\infty\}$ nous noterons leur birapport

$$\langle \alpha, \beta, \gamma, \delta \rangle := \frac{\alpha-\gamma}{\beta-\gamma} \Big/ \frac{\alpha-\delta}{\beta-\delta}.$$

Nous montrons, pour l'équation sous la forme (6), qu'il existe une fonction rationnelle explicite $V(a, b, c)$, (7), des racines qui donne une forme universelle simple de l'équation $Q(V) = 0$, des fonctions rationnelles $R_j(V)$ et des transformations rationnelles des racines de l'équation $Q(V) = 0$ en les reliant directement à l'action ci-dessus de S_3 sur l'espace projectif. On a

Théorème 2.1. *Considérons l'équation* (6).

(i) *L'équation $Q(V) = 0$ associée à la fonction rationnelle des trois racines de* (6),

$$V(a, b, c) = \frac{a-c}{b-c} = \langle a, b, c, \infty \rangle \tag{7}$$

est la suivante, où $\Omega = \frac{4s}{4s-1}$,

$$Q(V) = (1 - V + V^2)^3 - \frac{27}{4}\Omega V^2(1-V)^2. \tag{8}$$

(ii) *Les trois racines de l'équation* (6) *sont les fonctions rationnelles suivantes de* V,

$$R_1(V) = -\frac{V^2 - V + 1}{(V-2)(V+1)},$$
$$R_2(V) = \frac{V^2 - V + 1}{2(V - \frac{1}{2})(V+1)}, \quad R_3(V) = \frac{V^2 - V + 1}{2(V-2)(V - \frac{1}{2})}.$$

(iii) *Les transformations rationnelles des racines de* (8) *de la forme*

$$V \mapsto V(R_i(V), R_j(V), R_k(V)), \tag{9}$$

où (i, j, k) *est une permutation de* $(1, 2, 3)$*, sont données par l'action* (5) *du groupe symétrique* S_3 *dans l'espace projectif d'une clôture algébrique de* k.

Les six valeurs de V obtenues en permutant (a, b, c) en $(p(a), p(b), p(c))$ sont les six valeurs des birapports $\langle p(a), p(b), p(c), \infty\rangle$ et forment une orbite de l'action de S_3 sur $\mathbb{P}^1$ dont l'invariant est donné par Ω. On vérifie ensuite que la somme des $R_j(V)$ est égale à 0 et que la somme des $1/R_j(V)$ est égale à 3 alors que le produit vaut

$$\prod R_j(V) = -\frac{(V^2 - V + 1)^3}{(1-2V)^2(V-2)^2(V+1)^2}$$

ce qui donne

$$\frac{4s}{4s-1} = \frac{4(V^2 - V + 1)^3}{27(V-1)^2V^2} = \Omega.$$

On vérifie également que pour $V = \frac{a-c}{b-c}$ on a $R_1(V) = a$, en utilisant les relations $a + b + c = 0$ et $1/a + 1/b + 1/c = 3$. Les transformations (9) sont celles du birapport $\langle a, b, c, \infty\rangle$ quand on permute (a, b, c), i.e., plus précisément

$$\begin{pmatrix} \{1,2,3\} & \omega \\ \{1,3,2\} & 1-\omega \\ \{2,1,3\} & \frac{1}{\omega} \\ \{2,3,1\} & \frac{\omega-1}{\omega} \\ \{3,1,2\} & \frac{1}{1-\omega} \\ \{3,2,1\} & \frac{\omega}{\omega-1} \end{pmatrix}.$$

Comme la fonction $V(a, b, c)$ est invariante par le groupe affine on note que c'est aussi le cas pour les fonctions $R_j(V(a, b, c))$ qui ont donc comme propriété de normaliser le triplet (a, b, c) de telle sorte que sa somme soit nulle et que le barycentre des inverses soit égal à 1. Cette normalisation du triplet (a, b, c) est effectuée par une unique transformation affine et de plus celle-ci est à coefficients dans le corps des fonctions symétriques de (a, b, c).

Corollaire 2.2. *Soient $\alpha, \beta, \gamma, \delta \in K$ quatre éléments dont les birapports prennent six valeurs distinctes. Il existe une unique transformation projective $g \in PGL_2(K)$ telle que $g(\delta) = \infty$ et que*

$$g(\alpha) + g(\beta) + g(\gamma) = 0, \quad \frac{1}{3}\big(g(\alpha)^{-1} + g(\beta)^{-1} + g(\gamma)^{-1}\big) = 1 \tag{10}$$

De plus si ω désigne l'un des birapports de $\alpha, \beta, \gamma, \delta$, alors $\{g(\alpha), g(\beta), g(\gamma)\} \subset K$ est égal au sous-ensemble $\{R_j(\omega) \mid 1 \le j \le 3\} \subset K$.

L'existence résulte du Théorème 2.1. Pour montrer l'unicité on se ramène au cas $\delta = \infty$ et l'on voit que l'identité est la seule transformation affine qui préserve les conditions (10). La deuxième partie résulte du Théorème 2.1.

Nous montrons dans la Section 3 comment utiliser ce corollaire pour passer d'une racine à l'autre pour l'équation générale du quatrième degré.

Pour obtenir le groupe de Galois de l'équation (6) il faut décomposer le polynôme $Q(V)$ de (8) en facteurs irréductibles. On obtient facilement en utilisant l'action du sous-groupe $A_3 \subset S_3$ la factorisation

$$\begin{aligned} Q(X) &= (X^3 - tX^2 + (t-3)X + 1)(X^3 + (t-3)X^2 - tX + 1) \\ &= Q_1(X)Q_2(X) \end{aligned}$$

à condition que $t = \frac{3}{2}(1 \pm \sqrt{3}\sqrt{\Omega - 1})$. L'adjonction de t correspond à celle d'une racine carrée du discriminant $\Delta = 27s^2(4s-1)$ de (6).

Par construction le groupe A_3 agit sur les racines de l'équation $Q_1(X) = 0$ par la transformation d'ordre 3, $\omega \mapsto \frac{1}{1-\omega}$ et les racines donnent les trois branches $(\alpha(t), \beta(t), \gamma(t))$ de la fonction inverse de la fonction suivante

$$\Omega_1 := \frac{1 - 3\omega + \omega^3}{\omega(\omega - 1)}. \tag{11}$$

Remarque 2.3. Si le corps de base est contenu dans $\mathbb{R}$, les trois branches sont, pour $t \in \mathbb{R}$, réelles et définies sans ambiguité par les conditions $\alpha(t) > 1 > \beta(t) > 0 > \gamma(t)$. Alors α, β, γ donnent des isomorphismes analytiques croissants

$$\alpha\colon \mathbb{R} \to (1, \infty), \quad \beta\colon \mathbb{R} \to (0,1), \quad \gamma\colon \mathbb{R} \to (-\infty, 0).$$

On a

$$\beta(t) = 1 - \frac{1}{\alpha(t)}, \quad \gamma(t) = \frac{1}{1-\alpha(t)}, \quad \beta(t) + \beta(3-t) = 1, \quad \gamma(3-t) + \alpha(t) = 1$$

de plus $\alpha(t) = t - 1 + o(1)$ quand $t \to +\infty$ et $\gamma(t) = t - 1 + o(1)$ quand $t \to -\infty$.

On vérifie que, comme le groupe de Galois agit de manière rationnelle sur les racines de l'équation $Q_1(X)=0$, le discriminant Δ de Q_1 est un carré. On a $\Delta=(t^2-3t+9)^2$. Plus généralement la Proposition 2.4 donne la matrice de l'action du groupe de Galois dans la base $(1, X, X^2)$ en fonction de la racine carrée du discriminant, ce qui montre en particulier que si l'action du groupe de Galois est rationnelle le discriminant est un carré. Plus précisement, soient $p, q \in k$ et $P(X) := X^3 + pX + q \in k[X]$. Soient α, β, γ les racines de $P(X) = 0$ et Δ le discriminant de P :

$$\Delta = -4p^3 - 27q^2.$$

On suppose une fois pour toutes $\Delta \neq 0$, les racines sont donc distinctes.

Proposition 2.4. *Avec les notations ci-dessus, on a les égalités*

$$\beta, \gamma = -\frac{\alpha}{2} \pm \frac{-4p^2 + 9q\alpha - 6p\alpha^2}{2\sqrt{\Delta}}. \tag{12}$$

La matrice de l'automorphisme de Galois d'ordre 3 *de* $k(\sqrt{\Delta})[x]/P$ *est donnée par*

$$\begin{pmatrix} 1 & 0 & 0 \\ \frac{2p^2}{\sqrt{\Delta}} & -\frac{9q}{2\sqrt{\Delta}} - \frac{1}{2} & \frac{3p}{\sqrt{\Delta}} \\ \frac{3pq}{\sqrt{\Delta}} - p & \frac{p^2}{\sqrt{\Delta}} & \frac{9q}{2\sqrt{\Delta}} - \frac{1}{2} \end{pmatrix}.$$

On arrive facilement à ce résultat de la façon suivante : on a

$$\sqrt{\Delta} = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) = (\beta - \gamma)(\alpha^2 - \alpha(\beta + \gamma) + \beta\gamma) \tag{13}$$

et en utilisant $\alpha + \beta + \gamma = 0$ et $\alpha(\beta + \gamma) + \beta\gamma = p$, (13) donne

$$\sqrt{\Delta} = (\beta - \gamma)(3\alpha^2 + p)$$

d'où

$$\alpha + 2\beta = \frac{\sqrt{\Delta}}{3\alpha^2 + p}, \tag{14}$$

qui donne β en fonction rationnelle de $\alpha, p, q, \sqrt{\Delta}$ et se réécrit sous la forme (12) en utilisant $P(\alpha) = 0$ pour inverser $(3\alpha^2 + p)$ (i.e., $(3x^2 + p)$ dans $k(\sqrt{\Delta})[x]/P$) ce qui donne

$$\frac{1}{3\alpha^2 + p} = -\frac{1}{\Delta}(6p\alpha^2 - 9q\alpha + 4p^2), \tag{15}$$

(12) résulte alors de (14) et (15).

La matrice de l'automorphisme d'ordre 3 de $k(\sqrt{\Delta})[x]/P$ s'en déduit.

3. L'équation du quatrième degré

Il s'agit ci-dessous d'expliciter, comme dans la Proposition 2.4 dans le cas du 3-ème degré, l'action du groupe M_4 sur les racines d'une équation du quatrième degré, après adjonction du birapport des racines, laquelle réduit le groupe de Galois au groupe M_4. Cette réduction a lieu sauf quand les birapports des racines forment l'orbite $\{-1, \frac{1}{2}, 2\}$ (cas harmonique) ou $\{-j, -j^2\}$ (cas équiharmonique) et nous traitons séparément ces deux cas.

3.1. Rappels, formes binaires de degré 4. Cette section contient des rappels concernant les formes binaires, voir [3]. Considérons les formes binaires de degré 4 à coefficients dans k :

$$\phi(X,Y) = aX^4 + 4bX^3Y + 6cX^2Y^2 + 4dXY^3 + eY^4.$$

Elles constituent un k-espace vectoriel W de dimension 5. Le groupe $G = GL(2,k)$ opère naturellement sur $kX \oplus kY$ et donc dans W. L'annulation de ϕ définit un faisceau de 4 droites à condition de passer à la clôture algébrique $\overline{k}$ de k.

Considérons maintenant a, b, c, d, e comme des indéterminées. Dans $k[a,b,c,d,e]$ le groupe G agit naturellement. La sous-algèbre des invariants sous $SL(2,k)$ est engendrée par les polynômes I et J suivants, qui sont algébriquement indépendants

$$I = ae - 4bd + 3c^2, \quad J = \mathrm{Det}\begin{pmatrix} a & b & c \\ b & c & d \\ c & d & e \end{pmatrix}.$$

Considérons les G-orbites dans $W \setminus \{0\}$. Il y a 3 orbites exceptionnelles C_4, C_5, C_6 qui sont des cônes de dimensions $3, 3, 2$. Ignorons les désormais et supposons provisoirement $k = \overline{k}$. Les autres orbites sont des cônes de dimension quatre. Si on leur adjoint l'origine, ils sont fermés sauf un seul C_3 (dont le bord est $C_4 \cup C_5 \cup C_6$). Il y a trois cônes remarquables

- C_1 correspondant aux faisceaux harmoniques de quatre droites ;
- C_2 correspondant aux faisceaux équiharmoniques de quatre droites ;
- C_3 (déjà introduit) correspondant aux faisceaux qui ont une droite double.

La valeur de J^2/I^3 repère bijectivement les orbites de dimension quatre. Cette valeur est 0 sur C_1, ∞ sur C_2, $\frac{1}{27}$ sur C_3.

Le discriminant de ϕ est le discriminant, multiplié par a^6, du polynôme $\frac{1}{a}P(X)$, où

$$P(X) := aX^4 + 4bX^3 + 6cX^2 + 4dX + e. \tag{16}$$

Il vaut $\Delta = 2^8(I^3 - 27J^2)$.

Soient $\alpha, \beta, \gamma, \delta \in \overline{k}$ les inverses des pentes des quatre droites du faisceau. Ainsi $\alpha, \beta, \gamma, \delta$ sont aussi les racines du polynôme $P(X)$ de (16), avec une racine égale à ∞ si $a = 0$ (dans ce cas la droite $Y = 0$ fait partie du faisceau).

Les invariants I et J s'expriment en fonction de $\alpha, \beta, \gamma, \delta$: en posant

$$u = (\alpha - \beta)(\gamma - \delta), \quad v = (\alpha - \gamma)(\delta - \beta), \quad w = (\alpha - \delta)(\beta - \gamma),$$

on a alors ([3]),

$$I = \frac{a^2}{24}(u^2 + v^2 + w^2), \quad J = \frac{a^3}{432}(u - v)(v - w)(w - u).$$

Posons $K = k(\alpha, \beta, \gamma, \delta) \subset \overline{k}$. Pour a, b, c, d, e génériques K est une extension galoisienne de k de degré 24 de groupe de Galois S_4. Soit K_1, $k \subset K_1 \subset K$ le sous-corps des éléments de K invariants par A_4. On a $K_1 = k(\sqrt{\Delta})$. Définissons K_2, où $k \subset K_1 \subset K_2 \subset K$, comme le sous-corps des éléments de K invariants par M_4. C'est une extension galoisienne de degré 3 de K_1, et K est une extension galoisienne de K_2 de degré 4 et de groupe de Galois M_4.

Soient ω_j, $1 \leq j \leq 6$, les birapports de $\{\alpha, \beta, \gamma, \delta\}$, ils forment une orbite de l'action de S_3 sur $\mathbb{P}^1$ et soit Ω défini en (4), on a alors

$$\Omega = \frac{I^3}{I^3 - 27J^2} = 2^8 \frac{I^3}{\Delta}.$$

On a donc $K_1 = k(\sqrt{\Delta}) = k(\sqrt{3(\Omega - 1)}) = k(\Omega_1)$ avec Ω_1 défini en (11) .

Lemme 3.1. *Soient $\omega = \langle \alpha, \beta, \gamma, \delta \rangle$, $R_j(V)$ les trois fonctions du Théorème 2.1. On a*

$$\begin{aligned} \alpha\delta + \beta\gamma &= \frac{2c}{a} + 12\frac{J}{aI}R_1(\omega), \\ \alpha\gamma + \beta\delta &= \frac{2c}{a} + 12\frac{J}{aI}R_2(\omega), \\ \alpha\beta + \gamma\delta &= \frac{2c}{a} + 12\frac{J}{aI}R_3(\omega). \end{aligned} \tag{17}$$

Il s'agit d'un simple calcul en remplaçant dans I et J les termes a, b, c, d, e comme fonctions symétriques de $\{\alpha, \beta, \gamma, \delta\}$.

3.2. Action du groupe M_4 sur les racines. Soient $p, q, r \in k$ et

$$P(X) := X^4 + pX^2 + qX + r \in k[X].$$

On va étudier l'équation

$$P(X) = 0. \tag{18}$$

Soient $\alpha, \beta, \gamma, \delta$ les racines de (18), et Δ le discriminant de P. On a

$$\Delta = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3.$$

On suppose une fois pour toutes $\Delta \neq 0$, les racines sont donc distinctes.

L'invariant I de la forme homogénéisée de P est

$$I = r + 3\Big(\frac{p}{6}\Big)^2 = \frac{1}{12}(p^2 + 12r).$$

Donc la condition $p^2 + 12r = 0$ signifie que $\{\alpha, \beta, \gamma, \delta\}$ est équiharmonique. Ce cas sera traité dans Section 3.4. Pour l'instant on suppose

$$p^2 + 12r \neq 0.$$

L'invariant J de la forme homogénéisée de P est

$$J = \det\begin{pmatrix} 1 & 0 & p/6 \\ 0 & p/6 & q/4 \\ p/6 & q/4 & r \end{pmatrix} = 2^{-4}3^{-3}(-2p^3 + 72pr - 27q^2).$$

La condition $-2p^3 + 72pr - 27q^2 = 0$ signifie que $\{\alpha, \beta, \gamma, \delta\}$ est harmonique. Ce cas sera traité dans Section 3.3. Pour l'instant on suppose $-2p^3 + 72pr - 27q^2 \neq 0$.

On suppose $\alpha, \beta, \gamma, \delta$ génériques, $K = k(\alpha, \beta, \gamma, \delta)$ est une extension galoisienne de k de degré 24, de groupe de Galois S_4. Donc $k(\alpha)$ est loin d'être égal à K (même si l'on adjoint $\sqrt{\Delta}$).

Soient

$$\Big\{\omega, 1 - \omega, \frac{1}{\omega}, \frac{\omega - 1}{\omega}, \frac{1}{1 - \omega}, \frac{\omega}{\omega - 1}\Big\}$$

les birapports de $\alpha, \beta, \gamma, \delta$. Le corps $K_2 = k(\omega)$ est une extension galoisienne de k formée des éléments de K invariants sous M_4. Le corps K_2 est de degré 6 sur k et K de degré 4 sur K_2. Donc $K_2(\alpha) = K$, $K = k(\omega, \alpha)$. Le but est d'exprimer explicitement β, γ, δ en fonction rationnelle de p, q, r, ω, α.

Proposition 3.2. *L'action du groupe M_4 sur les racines $\alpha, \beta, \gamma, \delta$ est donnée par*

$$T_j(x) := x - P'(x)\Big(\frac{p}{3} + 12\frac{J}{I}R_j(\omega) + 2x^2\Big)^{-1}.$$

Montrons que la transformation T_1 vérifie

$$T_1(\alpha) = \delta, \quad T_1(\delta) = \alpha, \quad T_1(\beta) = \gamma, \quad T_1(\gamma) = \beta.$$

On a d'après (17),

$$\alpha\delta + \beta\gamma = \frac{p}{3} + 12\frac{J}{I}R_1(\omega).$$

Vue la symétrie de cette égalité, il suffit de montrer, que $T_1(\alpha) = \delta$, i.e., que

$$\delta = \alpha - P'(\alpha)/(\alpha\delta + \beta\gamma + 2\alpha^2).$$

Cela résulte de $P'(\alpha) = (\alpha - \beta)(\alpha - \gamma)(\alpha - \delta)$ et $\alpha + \beta + \gamma + \delta = 0$, d'où

$$(\alpha - \delta)(\alpha\delta + \beta\gamma + 2\alpha^2) = P'(\alpha).$$

3.3. Le cas harmonique. Dans cette section, on va analyser en grands détails le cas où $\{\alpha, \beta, \gamma, \delta\}$ est harmonique, i.e., $J = 0$. Alors $\Delta = 2^8 I^3$; la condition générale $\Delta \neq 0$ implique $I \neq 0$, et $K_1 = k(\sqrt{\Delta}) = k(\sqrt{I})$.

On note G_1 le groupe de Galois de K sur K_1, G le groupe de Galois de K sur k. On suppose bien entendu que P est irréductible sur k.

3.3.1. On reprend d'abord rapidement le cas général, sans hypothèse sur J. D'après la formule de Taylor, $\beta - \alpha, \gamma - \alpha, \delta - \alpha, \alpha - \alpha = 0$ sont solutions de

$$X^4 + 4\alpha X^3 + \sigma X^2 + \rho X + P(\alpha) = 0,$$

où $\rho = P'(\alpha)$, $\sigma = \frac{1}{2}P''(\alpha)$. Donc $1/(\beta - \alpha)$, $1/(\gamma - \alpha)$, $1/(\delta - \alpha)$ sont solutions de

$$X^3 + \frac{\sigma}{\rho}X^2 + \frac{4\alpha}{\rho}X + \frac{1}{\rho} = 0.$$

On pose

$$\beta' = \frac{\sigma}{3\rho} + \frac{1}{\beta - \alpha}, \quad \gamma' = \frac{\sigma}{3\rho} + \frac{1}{\gamma - \alpha}, \quad \delta' = \frac{\sigma}{3\rho} + \frac{1}{\delta - \alpha}.$$

Alors, d'une part, les birapports de $\{\alpha, \beta, \gamma, \delta\}$ sont égaux aux birapports de $\{\infty, \beta', \gamma', \delta'\}$, et d'autre part β', γ', δ' sont les solutions de

$$\Big(X - \frac{\sigma}{3\rho}\Big)^3 + \frac{\sigma}{\rho}\Big(X - \frac{\sigma}{3\rho}\Big)^2 + \frac{4\alpha}{\rho}\Big(X - \frac{\sigma}{3\rho}\Big) + \frac{1}{\rho} = 0.$$

Après quelques calculs, cette équation s'écrit

$$X^3 - \frac{4I}{\rho^2}X - \frac{16J}{\rho^3} = 0.$$

On en déduit

$$\beta' + \gamma' + \delta' = 0, \tag{19}$$

$$\beta'\gamma' + \beta'\delta' + \gamma'\delta' = -\frac{4I}{\rho^2}, \tag{20}$$

$$\beta'\gamma'\delta' = \frac{16J}{\rho^3}. \tag{21}$$

3.3.2. Dans toute la fin de cette Section 3.3, on suppose à nouveau $J = 0$. D'après (19), (20), (21), on a, à une permutation près de β', γ', δ',

$$\beta' = 0, \quad \gamma' = \frac{2\sqrt{I}}{\rho}, \quad \delta' = -\frac{2\sqrt{I}}{\rho}, \tag{22}$$

d'où

$$\frac{1}{\beta-\alpha} = -\frac{\sigma}{3\rho}, \quad \frac{1}{\gamma-\alpha} = -\frac{\sigma-6\sqrt{I}}{3\rho}, \quad \frac{1}{\delta-\alpha} = -\frac{\sigma+6\sqrt{I}}{3\rho}. \tag{23}$$

On en déduit d'abord

$$\sigma \neq 0, \quad \sigma \neq 6\sqrt{I}, \quad \sigma \neq -6\sqrt{I},$$

puis les formules suivantes qui permettent de passer de α aux trois autres racines

$$\beta = \alpha - \frac{3\rho}{\sigma}, \quad \gamma = \alpha - \frac{3\rho}{\sigma-6\sqrt{I}}, \quad \delta = \alpha - \frac{3\rho}{\sigma+6\sqrt{I}}, \tag{24}$$

3.3.3. On rappelle que G_1 est le groupe de Galois de K sur $K_1 = k(\sqrt{\Delta}) = k(\sqrt{I})$ et G celui de K sur k.

Lemme 3.3. *On suppose que $\{\alpha, \beta, \gamma, \delta\}$ est harmonique.*

(i) *On a $K = K_1(\alpha) = K_1(\beta) = K_1(\gamma) = K_1(\delta)$.*

(ii) *L'extension K de K_1 est galoisienne de degré 2 ou 4.*

(iii) *Si l'extension K de K_1 est de degré 4 son groupe de Galois G_1 est M_4 et il agit simplement transitivement sur $\{\alpha, \beta, \gamma, \delta\}$.*

Démonstration. (i) D'après (24) on a $\beta, \gamma, \delta \in K_1(\alpha)$. Donc $K = K_1(\alpha)$, ce qui entraine (i) car les raisonnements ci-dessus qui font jouer un rôle spécial à α s'appliquent à β, γ, δ.

(ii) Le (i) montre que l'extension K de K_1, qui est galoisienne par construction, est engendrée par α. Son degré $d \leq 4$ est divisible par 2 car $k(\alpha) \subset K$ donc 4 divise $2d$.

(iii) Comme K_1 contient $\sqrt{\Delta}$ et K est engendré par α le groupe G_1 est contenu dans le groupe alterné A_4. Or celui-ci contient un seul sous-groupe d'ordre 4, à savoir M_4. Comme l'extension K de K_1 est galoisienne G_1 agit transitivement sur $\{\alpha, \beta, \gamma, \delta\}$ et comme G_1 est d'ordre 4 cette action est simplement transitive. ∎

3.3.4. Notons $S \subset S_4$ le sous-groupe formé en adjoignant à $M_4 \subset S_4$ une transposition $s, s^2 = 1$. Ce sous-groupe est unique à conjugaison près et est un sous-groupe de Sylow associé au nombre premier $p = 2$.

Proposition 3.4. *On suppose que* $\{\alpha, \beta, \gamma, \delta\}$ *est harmonique.*

(i) *Si le discriminant* Δ *n'est pas un carré dans* k *et si l'extension* K *de* K_1 *est de degré* 4*, le groupe de Galois* G *de* K *sur* k *est d'ordre* 8*, conjugué à* S*.*

(ii) *Si les conditions de* (i) *ne sont pas vérifiées, l'extension* K *de* k *est de degré* 4*, égale à* $k(\alpha)$*.*

Démonstration. (i) L'extension K_1 est de degré 2 sur k et K de degré 4 sur K_1, donc l'extension galoisienne K de k est de degré 8. Le sous-groupe S est, à conjugaison près, le seul sous-groupe d'ordre 8 dans S_4 (par le théorème de Sylow).

(ii) Si les conditions de (i) ne sont pas vérifiées, on a soit $K_1 = k$ et le Lemme 3.3 montre que $K = k(\alpha)$, soit l'extension K de K_1 est de degré 2 et donc de degré 4 sur k de sorte que $K = k(\alpha)$. ∎

3.3.5. Exemples. Soit $P(x) = x^4 - \frac{15x^2}{2} + 5x + \frac{5}{16}$. On vérifie que l'on a $J = 0$, de plus l'extension associée est galoisienne de groupe de Galois $\mathbb{Z}/4\mathbb{Z}$. On a

$$P(x) = \left(x^2 + \sqrt{5}x - \frac{1}{4}(2\sqrt{5} + 5)\right)\left(x^2 - \sqrt{5}x - \frac{1}{4}(5 - 2\sqrt{5})\right).$$

Le corps K est l'extension quadratique de $K_1 = \mathbb{Q}(\sqrt{5})$ obtenue en adjoignant une racine carrée de $z = 10 + 2\sqrt{5}$. L'extension de l'automorphisme de $\mathbb{Q}(\sqrt{5})$ au corps K admet pour carré l'automorphisme de Galois de K sur $\mathbb{Q}(\sqrt{5})$ qui change z en $-z$, ce qui montre que $G = \mathbb{Z}/4\mathbb{Z}$.

Le polynôme $P(x) = x^4 + 6x^2 + 1$ donne un exemple où $J = 0$, $\Delta = 2^{14}$ est un carré, et le groupe G est égal à M_4 (Lemme 3.3 (iii)).

3.3.6. Si $p = 0$ la condition $J = 0$ donne $q = 0$ et $P(X) = X^4 + r$. On a $I = r$.

Si k contient $i = \sqrt{-1}$ l'extension galoisienne K est égale à $k[X]/P(X)$, son groupe de Galois est le groupe $G = \mathbb{Z}/4$ engendré par $X \mapsto iX$. Le sous-corps $K_1 = k(\sqrt{I})$ est le sous-corps de $k[X]/P(X)$ formé des polynômes pairs. Le corps K est de dimension 2 sur K_1.

Si le polynôme $X^2 + 1$ est irreducible sur k, l'extension galoisienne K est égale à $k(i)[X]/P(X)$, elle est de degré 8 sur k. Le groupe de Galois G de K sur k s'identifie au groupe diédral $D = \mathbb{Z}/4 \rtimes \mathbb{Z}/2$, où l'action de $\mathbb{Z}/4$ sur $k(i)[X]/P(X)$ est donnée par $X \mapsto i^k X$ et celle du générateur de $\mathbb{Z}/2$ par la conjugaison $i \mapsto -i$ sur $k(i)$. Ce groupe D est isomorphe à $S = M_4 \rtimes \mathbb{Z}/2$. Le sous-corps $K_1 = k(\sqrt{I})$ est engendré par l'élément $iX^2 \in k(i)[X]/P(X)$. Le sous-groupe $G_1 \subset G$ qui fixe iX^2 est engendré par l'élément d'ordre 2 de $\mathbb{Z}/4 \subset D$ et $1 \in \mathbb{Z}/2 \subset D$, il est isomorphe à M_4.

3.3.7. Supposons $p \neq 0$. On utilise l'égalité $J = 0$ pour exprimer r en fonction de p, q, i.e.,

$$r = \frac{2p^3 + 27q^2}{72p}.$$

On peut calculer la matrice Σ, dans la base $1, X, X^2, X^3$ de l'automorphisme ϕ de $k[X]/P(X)$ qui provient de la transformation $\alpha \mapsto \beta$ de (24). On obtient en utilisant $I = \frac{p^2}{9} + \frac{3q^2}{8p} \neq 0$,

$$\begin{aligned}(25)\qquad \Sigma = {} & \frac{1}{8p^3 + 27q^2} \\ & \times \begin{pmatrix} 8p^3 + 27q^2 & 0 & 0 & 0 \\ -18p^2q & -3(16p^3 + 9q^2) & 36pq & -48p^2 \\ -8p^4 - 54pq^2 & -60p^2q & 27q^2 - 8p^3 & -72pq \\ 9p^3q - \frac{81q^3}{2} & \frac{140p^4}{3} & -42p^2q & 48p^3 - 27q^2 \end{pmatrix}\end{aligned}$$

et l'on vérifie directement que $\Sigma^2 = 1$ et que le déterminant de Σ vaut 1. On obtient de même la matrice Σ' associée à la transformation $\alpha \mapsto \gamma$. On a, comme $I = \frac{p^2}{9} + \frac{3q^2}{8p} \neq 0$,

$$(26)\qquad (8p^3 + 27q^2)\Sigma'$$

$$= \begin{pmatrix} 8p^3 + 27q^2 & 0 & 0 & 0 \\ \frac{9}{2}pq(2p - \sqrt{I}) & p^2(20p - 7\sqrt{I}) & -18pq & 6p(4p - \sqrt{I}) \\ p^3(\sqrt{I} - 4p) & -3pq(\sqrt{I} - 10p) & 2p^2\sqrt{I} - 27q^2 & 36pq \\ -\frac{3}{4}q(-6p^2\sqrt{I} + 22p^3 + 27q^2) & \sqrt{I}\left(\frac{35p^3}{6} - \frac{9q^2}{4}\right) - \frac{70p^4}{3} & \frac{3}{2}pq(\sqrt{I} + 14p) & p^2(5\sqrt{I} - 28p) \end{pmatrix}$$

et l'on vérifie que $\Sigma'^2 = 1$ et que $\Sigma\,\Sigma' = \Sigma'\,\Sigma$.

Si $\sqrt{I} \in k$ (i.e., $\sqrt{\Delta} \in k$) la formule (26) définit un automorphisme ϕ' de $k[X]/P(X)$ et ϕ, ϕ' donnent l'action de M_4 sur cette extension galoisienne de k.

Quand l'extension galoisienne K de k est de degré 8, on est dans le cas (i) de la Proposition 3.4, l'extension K est obtenue en adjoignant $\sqrt{I}$ au corps $k[X]/P(X)$ et nous l'identifions avec $k(\sqrt{I})[X]/P(X)$. Elle admet une involution unique θ qui est l'identité sur $k[X]/P(X)$ et telle que $\theta(\sqrt{I}) = -\sqrt{I}$. De plus comme $I \in k$, l'automorphisme ϕ de $k[X]/P(X))$ se prolonge à K en fixant $\sqrt{I}$. La matrice Σ' est une matrice à coefficients dans $k(\sqrt{I})$ et définit un automorphisme ϕ' de K fixant $\sqrt{I}$. On obtient ainsi la description du groupe de Galois comme produit semi-direct S de M_4, qui agit par ϕ, ϕ' et de l'involution θ qui transforme ϕ' en son inverse.

Supposons maintenant que K est de dimension 4 sur k et $\sqrt{I} \notin k$. On identifie K avec $k[X]/P(X)$. L'équation $X^2 = I$ admet ses racines $\pm\xi(X) \in k[X]/P(X)$ dans le corps K et celles-ci engendrent le corps $K_1 \subset K$. L'automorphisme ϕ de K donné par la matrice Σ permute les racines $\alpha, \beta, \gamma, \delta \in k[X]/P(X)$ et comme $\phi(\alpha) = \beta$ et la permutation est paire car le déterminant de Σ vaut 1, on a $\phi(\gamma) = \delta$. La matrice Σ' n'a plus de sens en tant que transformation de K, mais il reste vrai que les quatre racines de $P(X) = 0$ qui forment une base de K sur k vérifient (23), d'où

$$\frac{1}{\gamma - \alpha} - \frac{1}{\delta - \alpha} = \frac{4\sqrt{I}}{\rho}$$

d'où, en utilisant $\rho = (\alpha - \beta)(\alpha - \gamma)(\alpha - \delta)$ on déduit

$$4\sqrt{I} = -(\alpha - \beta)(\alpha - \delta) + (\alpha - \beta)(\alpha - \gamma) = (\alpha - \beta)(\delta - \gamma)$$

et il en résulte, comme la permutation des racines associée à ϕ est

$$(\alpha, \beta, \gamma, \delta) \mapsto (\beta, \alpha, \delta, \gamma),$$

que $\phi(\sqrt{I}) = \sqrt{I}$. Ainsi le sous-corps $K_1 = k(\sqrt{I})$ est le corps fixe de ϕ. Comme K est une extension galoisienne de k l'automorphisme ψ: $\sqrt{I} \mapsto -\sqrt{I}$ de K_1 se prolonge en un automorphisme $\widetilde{\psi}$ de K. Montrons que la permutation correspondante des racines est soit η: $(\alpha, \beta, \gamma, \delta) \mapsto (\gamma, \delta, \beta, \alpha)$ soit η': $(\alpha, \beta, \gamma, \delta) \mapsto (\delta, \gamma, \alpha, \beta)$. La condition d'harmonicité réduit le groupe des permutations possibles à 8 permutations parmi lesquelles seules 4 sont impaires, et donc transforment $\sqrt{I}$ en $-\sqrt{I}$. Les permutations η, η' transforment le birapport des racines en son inverse ce qui est compatible avec la condition d'harmonicité. Elles transforment $(\alpha - \beta)(\delta - \gamma)$ en son opposé, et donc $\sqrt{I}$ en $-\sqrt{I}$. Mais ces deux propriétés sont également vérifiées par les deux permutations

$$(\alpha, \beta, \gamma, \delta) \mapsto (\beta, \alpha, \gamma, \delta) \quad \text{et} \quad (\alpha, \beta, \gamma, \delta) \mapsto (\alpha, \beta, \delta, \gamma).$$

La raison pour laquelle celles-ci sont exclues est la transitivité du groupe de Galois sur les racines. En effet le groupe de permutations obtenues en incluant ϕ préserverait la partition des racines en $\{\alpha, \beta\} \cup \{\gamma, \delta\}$ ce qui est exclu car le polynôme $P(X)$ est irréductible sur k. On a alors, toujours sous les hypothèses $J = 0$, $p \neq 0$, le théorème suivant.

Théorème 3.5. *Si l'extension K de $k(\sqrt{\Delta})$ est de degré 2, on a $K \sim k[X]/P(X)$ et le groupe de Galois de l'extension K de k est le groupe $\mathbb{Z}/4$. Le sous-corps $k(\sqrt{\Delta})$ est le corps des points fixes de l'automorphisme involutif ϕ donné par la matrice Σ de* (25).

La Proposition 3.4 montre que $K \sim k[X]/P(X)$. Comme $\beta' = 0$ et $\gamma' + \delta' = 0$ par (22), on a $\langle \alpha, \beta, \gamma, \delta \rangle = -1$. Le raisonnement ci-dessus montre que la permutation $\widetilde{\psi}$ des racines est soit

$$(\alpha, \beta, \gamma, \delta) \mapsto (\gamma, \delta, \beta, \alpha) \quad \text{soit} \quad (\alpha, \beta, \gamma, \delta) \mapsto (\delta, \gamma, \alpha, \beta).$$

Dans les deux cas le carré de ψ est égal à ϕ et le groupe de Galois est $\mathbb{Z}/4$.

3.4. Le cas équiharmonique. Pour simplifier, on suppose que k contient les trois racines de l'équation $X^3 = 1$. On note $j \in k$, $j \neq 1$, une racine cubique de l'unité, on a $j - j^2 = i\sqrt{3}$. Soit $P(X)$ équiharmonique. On a $I = 0$ donc $J \neq 0$, $2^{-8}\Delta = -27J^2 = (3i\sqrt{3}\,J)^2$ donc $\sqrt{\Delta} \in k$, $K_1 = k(\sqrt{\Delta}) = k$. Les équations de Section 3.3.1 montrent que $\beta', \gamma', \delta' \neq 0$ et, après permutation éventuelle de γ', δ', que $\gamma' = j\beta'$, $\delta' = j^2\beta'$ et $\beta'^3 = 16J/\rho^3$. Soit $\sqrt[3]{2J} \in \bar{k}$ la racine cubique de $2J$ égale à $\frac{1}{2}\rho\beta'$. On a $\sqrt[3]{2J} \in K$. Posons $K_1' = k(\sqrt[3]{2J})$. C'est une extension galoisienne de k de groupe de Galois $\mathbb{Z}/3$ ou $\{e\}$. On a, après une permutation éventuelle de $\{\beta', \gamma', \delta'\}$,

$$\beta' = 2\frac{\sqrt[3]{2J}}{\rho}, \quad \gamma' = 2j\frac{\sqrt[3]{2J}}{\rho}, \quad \delta' = 2j^2\frac{\sqrt[3]{2J}}{\rho},$$
$$(\beta - \alpha)^{-1} = \beta' - \frac{\sigma}{3\rho} = \frac{1}{3\rho}(6\sqrt[3]{2J} - \sigma),$$
$$\beta = \alpha + \frac{3\rho}{6\sqrt[3]{2J} - \sigma}, \quad \gamma = \alpha + \frac{3\rho}{6j\sqrt[3]{2J} - \sigma}, \quad \delta = \alpha + \frac{3\rho}{6j^2\sqrt[3]{2J} - \sigma}.$$

On a donc $K = K_1'(\alpha)$ et le degré de l'extension K de K_1' est ≤ 4.

Proposition 3.6. *On suppose $j \in k$. Soit $P(X)$ équiharmonique. Alors $\sqrt{\Delta} \in k$ et deux cas sont possibles :*

(1) *$K_1' = k$. Le groupe de Galois de K sur k est M_4 ;*

(2) *$K_1' \neq k$. Alors K_1' est extension galoisienne de k de groupe $\mathbb{Z}_3$, K est extension galoisienne de K_1' de groupe M_4 et extension galoisienne de k de groupe A_4.*

Si $K_1' = k$ le degré de K sur k est égal à 4, le groupe de Galois de K sur k est le seul sous-groupe de A_4 d'ordre 4. Si $K_1' \neq k$, K_1' est extension galoisienne de k de groupe $\mathbb{Z}_3$, comme le degré de K sur k est divisible par 4 car $k(\alpha) \subset K$, l'extension galoisienne K de K_1' est necessairement de degré 4 et son groupe de Galois est M_4. Le groupe de Galois de K sur k est le groupe A_4.

Il est facile de donner des exemples de ce deuxième cas. Un exemple du premier cas est donné par le polynôme $P(x) = x^4 - 3x^2 + 3x - \frac{3}{4}$ sur $k = \mathbb{Q}(j)$. On vérifie que dans ce cas $I = 0$ et $2J = -\frac{1}{8}$. Son groupe de Galois sur $k = \mathbb{Q}(j)$ est M_4 et son groupe de Galois sur $\mathbb{Q}$ est un sous-groupe de Sylow d'ordre 8 de S_4.

e

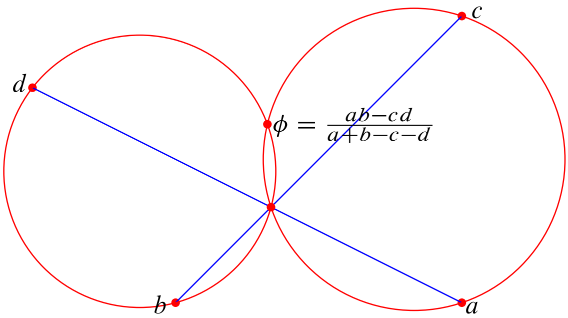

Figure 1

Les deux cercles (a, c, e) et (b, d, e) se recoupent en ϕ.

4. L'ange de la géométrie et le diable de l'algèbre

4.1. Lagrange. On trouve à la fin de l'article de Lagrange [4] sur l'équation du quatrième degré, dans sa discussion de l'article de Bezout de 1762, la fonction rationnelle suivante des quatre racines (a, b, c, d) qui ne prend que trois valeurs différentes quand on permute les racines :

$$\varphi(a, b, c, d) = \frac{ab - cd}{a + b - c - d}. \tag{27}$$

Cette expression est rationnellement équivalente à la fonction classique

$$\psi(a, b, c, d) = ab + cd$$

et l'on vérifie par un calcul direct, en notant s_j les fonctions symétriques des racines, les égalités

$$\varphi = \frac{s_1\psi - 2s_3}{4\psi + s_1^2 - 4s_2}, \quad \psi = \frac{(s_1^2 - 4s_2)\varphi + 2s_3}{s_1 - 4\varphi}.$$

L'expression (27) est covariante pour l'action du groupe affine, i.e., on a pour $g(z) = \lambda z + \mu$, $\lambda \neq 0$,

$$\varphi(g(a), g(b), g(c), g(d)) = g(\varphi(a, b, c, d)).$$

Cette covariance indique que le point $\varphi(a, b, c, d)$ doit s'interpréter géométriquement dans le plan complexe. Nous donnons une interprétation géométrique de $\varphi(a, b, c, d)$.

Proposition 4.1. *Soient $a, b, c, d \in \mathbb{C}$. Le point $\varphi(a, b, c, d) \in \mathbb{C}$ est le point d'intersection des quatre cercles circonscrits aux triangles (a, c, e), (b, d, e), (a, d, f), (b, c, f), où e est l'intersection des diagonales (ad) et (bc) et f l'intersection des diagonales (ac) et (bd).*

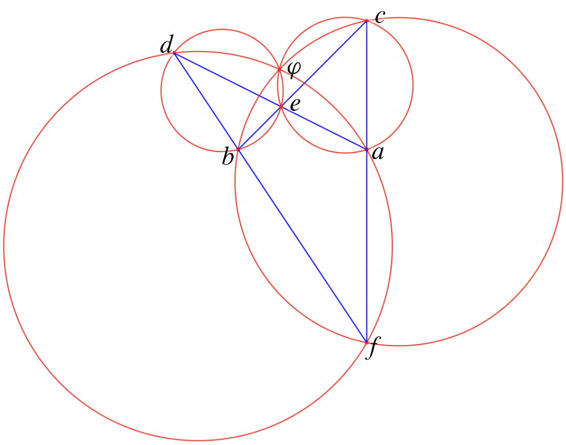

FIGURE 2
Le point φ est l'intersection des cercles (a, c, e), (b, d, e), (a, d, f), (b, c, f).

Il suffit de démontrer que le point φ est le deuxième point d'intersection des cercles circonscrits aux triangles (a, c, e), (b, d, e). Voir Figures 1 et 2. On utilise la covariance pour le groupe affine qui permet de supposer que $e = 0$. Une inversion de centre e (plus précisément l'application $z \mapsto 1/z$ du plan complexe), réduit alors l'égalité à un calcul simple.

4.2. Morley.

4.2.1. Dans cette section nous montrons comment généraliser le théorème de Morley (Figure 3) dans le cadre des équations du 3-ème et du 4-ème degré. Le point de départ est la démonstration [2] du théorème de Morley utilisant les nombres complexes. La résolvante donnée par le birapport $\langle a, b, c, \infty \rangle$ du Théorème 2.1 joue un rôle crucial dans notre généralisation. L'idée de [2] consiste à décrire les sommets du triangle de Morley comme points fixes du produit de deux rotations autour des sommets A, B, C d'un triangle et d'observer que le produit des cubes de ces rotations est l'identité. On utilise alors un lemme algébrique général sur le groupe $H(K)$ des transformations d'un corps K de la forme

$$x \mapsto g(x) = \alpha x + \beta,$$

où $\alpha, \beta \in K, \alpha \neq 0$ et le morphisme de groupe $\chi \colon H(K) \to K^{\times}$ qui associe à $g \in H(K)$ l'élément $\chi(g) = \alpha \in K^{\times}$. Si $\chi(g) \neq 1$ on note $\mathrm{fix}(g)$ l'unique point fixe de g, i.e., $x \in K$ tel que $g(x) = x$. Le lemme est le suivant.

Lemme 4.2 ([2]). *Soient $f, g, h \in H(K)$ tels que $f^3 g^3 h^3 = 1$ et que $j := \chi(fgh) \neq 1$. On suppose que f^3, g^3 et h^3 ne sont pas des translations. Alors fg, gh et hf ne sont pas des translations et*

$$\mathrm{fix}(fg) + j\ \mathrm{fix}(gh) + j^2\,\mathrm{fix}(hf) = 0.$$

Comme $f^3 g^3 h^3 = 1$ on a $j^3 = 1$ et j est donc une racine cubique primitive de 1 dans K.

Remarque 4.3. Soient $a, b, c \in K$, les conditions suivantes sont équivalentes :

(1) Il existe $j \neq 1$, $j^3 = 1$, tel que $a + jb + j^2 c = 0$;

(2) Il existe $j \neq 1$, $j^3 = 1$, tel que $\langle a, b, c, \infty \rangle = -j$;

(3) La configuration a, b, c, ∞ est équiharmonique.

Quand $K = \mathbb{C}$, les conditions précédentes signifient que le triangle (a, b, c) est équilatère.

Soient $z \in \mathbb{P}^1(K)$, $H_z \subset \mathrm{PGL}_2(K)$ le sous-groupe des éléments qui fixent z. L'application $\chi_z \colon H_z \to K^\times$ définie par

$$\chi_z(f) = \chi(hfh^{-1})$$

indépendament du choix de $h \in \mathrm{PGL}_2(K)$ tel que $h(z) = \infty$ est un morphisme de groupe canonique $\chi_z \colon H_z \to K^\times$. On note $\ker(\chi_z)$ le noyau de χ_z. Soit $f \in H_z$ tel que $\chi_z(f) \neq 1$, on note $\mathrm{fix}_{\neq z}(f) \in P^1(K)$ l'autre point fixe de f.

Corollaire 4.4. *Soient $z \in P^1(K)$, $f, g, h \in H_z$ tels que $f^3 g^3 h^3 = \mathrm{Id}$ et que $j := \chi_z(fgh) \neq 1$. On suppose que f^3, g^3 et h^3 ne sont pas dans $\ker(\chi_z)$. Alors fg, gh et hf ne sont pas dans $\ker(\chi_z)$ et la configuration $(z, \mathrm{fix}_{\neq z}(fg), \mathrm{fix}_{\neq z}(gh), \mathrm{fix}_{\neq z}(hf))$ est équiharmonique.*

On se ramène par conjugaison par un élément de $\mathrm{PGL}_2(K)$ au cas où $z = \infty$ et on applique le Lemme 4.2 et la Remarque 4.3.

4.2.2. Soient K un corps contenant une racine cubique de l'unité, $j \neq 1$, et $\sigma \in \mathrm{Aut}(K)$ un automorphisme de K, tel que $\sigma^2 = \mathrm{Id}$ et que $\sigma(j) = j^2$. Soit $H = H(K)$ le groupe affine de K, on note $h(\alpha, \beta) \in H(K)$ l'élément tel que

$$h(\alpha, \beta)(x) = \alpha x + \beta,$$

pour tout $x \in K$. Soit $\widetilde{H} = H \rtimes_\sigma \mathbb{Z}/2$ le produit semi-direct de H par l'automorphisme σ. Ses éléments sont de la forme $h(\alpha, \beta)$ ou $h(\alpha, \beta)\sigma$ avec $\sigma^2 = 1$, $\sigma h(\alpha, \beta) = h(\sigma(\alpha), \sigma(\beta))\sigma$. Le corps K est un espace vectoriel de dimension 2 sur le sous-corps K^σ des points fixes de σ.

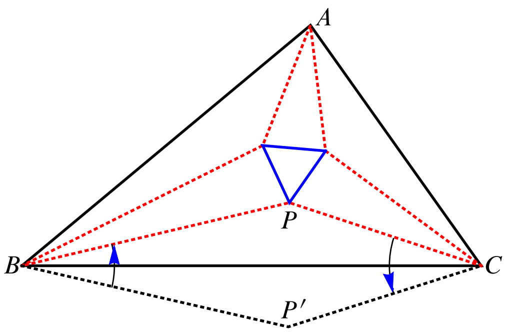

FIGURE 3
Le point P, intersection des trisectrices issues de B et C, est le point fixe du produit $R_B R_C$ de rotations de centre B et C. On a $R_A^3 R_B^3 R_C^3 = 1$.

Lemme 4.5. *Soient K et J comme ci-dessus.*

(i) *Soient $a, b \in K$, $a \neq b$. L'égalité*

$$s(a,b) = h\left(\frac{a-b}{\sigma(a)-\sigma(b)}, \frac{a\sigma(b)-b\sigma(a)}{\sigma(b)-\sigma(a)}\right)\sigma$$

définit une involution, $s(a,b)^2 = 1$ dont les point fixes forment la droite passant par a et b dans le plan $K \sim (K^\sigma)^2$.

(ii) *Soient $a, b, c \in K$ trois éléments distincts non-alignés sur K^σ, $\omega = \langle a, b, c, \infty\rangle$. Le produit $s(a,c)s(b,c)$ est l'unique élément $g \in H$ qui fixe le point c et tel que*

$$\chi(g) = \omega/\sigma(\omega).$$

(iii) *Soit $g \in H$ comme dans* (ii)*. On a $g = h(\chi(g), x)$, où $x = c - c\omega/\sigma(\omega)$.*

Démonstration. (i) L'unique élément g de H tel que $g(a) = 0$ et $g(b) = 1$ est

$$h\left(\frac{1}{b-a}, -\frac{a}{b-a}\right).$$

On a

$$s(a,b) = g^{-1}\sigma g.$$

On est donc ramené au cas où $a = 0, b = 1$ et dans ce cas l'involution σ a bien pour points fixes la droite du plan $K \sim (K^\sigma)^2$ passant par $a = 0, b = 1$.

(ii) Par construction $s(a,c)$ et $s(b,c)$ fixent c. Le calcul du produit montre que l'élément $s(a,c)s(b,c)$ de H est de la forme indiquée. Comme a, b, c sont non-alignés on a $\omega \neq \sigma(\omega)$ et l'unicité de x tel que $h(\omega/\sigma(\omega), x) = s(a,c)s(b,c)$ en résulte.

(iii) Comme $g(c) = c$ et $\chi(g) = \omega/\sigma(\omega)$, on a $x = c - c\omega/\sigma(\omega)$. ∎

Notons,

$$\theta(a,b;c) := h(\omega/\sigma(\omega), c - c\omega/\sigma(\omega)), \quad \omega := \langle a,b,c,\infty\rangle. \tag{28}$$

Lemme 4.6. *Soient $a,b,c \in K$ trois éléments distincts non-alignés sur K^σ. On a*

$$\theta(a,b;c)\theta(c,a;b)\theta(b,c;a) = \mathrm{Id}. \tag{29}$$

Cela résulte des simplifications suivantes

$$(s(a,c)s(b,c))(s(b,c)s(a,b))(s(a,b)s(a,c)) = s(a,c)s(a,c) = \mathrm{Id}.$$

Si $\omega = \langle a,b,c,\infty\rangle$ le produit des trois birapports impliqués dans (4.6) est

$$\omega \cdot \frac{1}{1-\omega} \cdot \frac{\omega-1}{\omega} = -1$$

et donc le produit des rapports avec les transformés par σ vaut bien 1.

Pour $x,y \in \mathbb{P}^1(K)$, $x \neq y$, et $u \in K^\times$ on note $\rho(u;x,y)$ l'unique élément g de $H_y(K)$ tel que $g(x) = x$ et que $\chi_y(g) = u$.

Corollaire 4.7. *Soient $\alpha,\beta,\gamma,\delta \in K$ quatre éléments distincts, $\omega = \langle\beta,\gamma,\delta,\alpha\rangle \notin K^\sigma$. On note*

$$\omega' = \frac{1}{1-\omega}, \quad \omega'' = \frac{\omega-1}{\omega}.$$

On a alors

$$\rho(\omega/\sigma(\omega);\delta,\alpha)\rho(\omega'/\sigma(\omega');\gamma,\alpha)\rho(\omega''/\sigma(\omega'');\beta,\alpha) = \mathrm{Id}. \tag{30}$$

Supposons d'abord $\alpha = \infty$, on a alors, en utilisant (28), avec $a = \beta, b = \gamma, c = \delta$ les égalités

$$\rho(\omega/\sigma(\omega);\delta,\alpha) = \theta(a,b;c),$$
$$\rho(\omega'/\sigma(\omega');\gamma,\alpha) = \theta(c,a;b), \quad \rho(\omega''/\sigma(\omega'');\beta,\alpha) = \theta(b,c;a),$$

ainsi que $\omega = \langle a,b,c,\infty\rangle$ et (30) se déduit du Lemme 4.6. Supposons $\alpha \neq \infty$. On a pour tout $h \in \mathrm{PGL}_2(K)$, $x,y \in \mathbb{P}^1(K)$, $x \neq y$, et $u \in K^\times$ l'égalité

$$\rho(u;h(x),h(y)) = h\,\rho(u;x,y)\,h^{-1}.$$

Soit $h \in \mathrm{PGL}_2(K)$ la transformation projective $h(z) := (z-\alpha)^{-1}$. Soient

$$a = h(\beta), \quad b = h(\gamma), \quad c = h(\delta).$$

On a

$$\omega = \langle\beta,\gamma,\delta,\alpha\rangle = \langle a,b,c,\infty\rangle$$

et les trois termes du produit (30) sont les conjugués par h des trois termes de (29) et on obtient (30) grâce au Lemme 4.6.

4.2.3. Racines cubiques des birapports. Soit

$$\varpi = \left\{\omega, 1-\omega, \frac{1}{\omega}, \frac{\omega-1}{\omega}, \frac{1}{1-\omega}, \frac{\omega}{\omega-1}\right\}$$

une orbite pour l'action du groupe symétrique S_3 sur l'espace projectif $\mathbb{P}^1(K)$.

Définition 4.8. Une racine cubique $\sqrt[3]{\varpi}$ de ϖ est le choix $u \mapsto \sqrt[3]{u}$ d'une racine cubique pour chacun des éléments de ϖ tel que

- si $u, v \in \varpi$ vérifient $uv = 1$ alors $\sqrt[3]{u}\,\sqrt[3]{v} = 1$;
- si $u, v, w \in \varpi$ vérifient $uvw = -1$ alors $\sqrt[3]{u}\,\sqrt[3]{v}\,\sqrt[3]{w} \neq -1$.

On vérifie que, dans le cas général, ϖ admet 18 racines cubiques, qui sont des applications de ϖ dans $\overline{k}$.

4.2.4. Généralisation du théorème de Morley. On utilise les notations k, K, j, σ ci-dessus. On prolonge σ en un automorphisme (pas nécessairement involutif) de la clôture algébrique $\overline{k} \supset K$ de k. Soit $u \in \overline{k}$, $u \notin \{0, 1\}$. Soient $\alpha, \beta \in \mathbb{P}^1(K)$, $\alpha \neq \beta$. Il existe un unique élément de $\mathrm{PGL}_2(\overline{k})$ qui fixe α et β et tel que u soit l'élément correspondant du groupe multiplicatif $G_m(\overline{k})$ (par conjugaison par une transformation projective transformant α en 0 et β en ∞). On note, comme ci-dessus, cet élément $\rho(u; \alpha, \beta)$. On a $\rho(u; \beta, \alpha) = \rho(u^{-1}; \alpha, \beta)$. Compte tenu de la Remarque 4.3, le théorème suivant est une généralisation du théorème de Morley.

Théorème 4.9. *Soient $\alpha, \beta, \gamma, \delta \in K$ quatre éléments distincts dont les birapports prennent six valeurs distinctes hors de K^σ. Soit $\sqrt[3]{\varpi}$ une racine cubique de ces birapports. Posons*

$$u = \langle \beta, \gamma, \delta, \alpha \rangle^{1/3}, \quad v = \langle \delta, \beta, \gamma, \alpha \rangle^{1/3}, \quad w = \langle \gamma, \delta, \beta, \alpha \rangle^{1/3}$$

(les valeurs des racines cubiques étant spécifiées par $\sqrt[3]{\varpi}$). Soient

$$\phi = \rho(u/\sigma(u); \delta, \alpha), \quad \psi = \rho(v/\sigma(v); \gamma, \alpha), \quad \chi = \rho(w/\sigma(w); \beta, \alpha).$$

Alors la configuration $(\alpha, \mathrm{fix}_{\neq\alpha}(\phi\psi), \mathrm{fix}_{\neq\alpha}(\psi\chi), \mathrm{fix}_{\neq\alpha}(\chi\phi))$ *est* équiharmonique.

En effet, le Corollaire 4.7 montre que l'on a $\phi^3\psi^3\chi^3 = \mathrm{Id}$. On applique alors le Corollaire 4.4 en utilisant la deuxième condition de la Définition 4.8 pour assurer que les hypothèses sont vérifiées. Il en résulte que la configuration

$$(\alpha, \mathrm{fix}_{\neq\alpha}(\phi\psi), \mathrm{fix}_{\neq\alpha}(\psi\chi), \mathrm{fix}_{\neq\alpha}(\chi\phi))$$

est équiharmonique.

Remerciements. Nous remercions le rapporteur pour ses judicieuses observations.

Références

[1] R. Bourgne and J-P. Azra (eds.), *Écrits et mémoires mathématiques d'Évariste Galois*. Gauthier-Villars, Paris, 1962. Zbl 0192.01502 MR 0150016

[2] A. Connes, A new proof of Morley's theorem. In *Les relations entre les mathématiques et la physique théorique*, pp. 43–46, Institut des Hautes Études Scientifiques, Bures-sur-Yvette, 1998. Zbl 1006.51010 MR 1667897

[3] E. Elliott, *An introduction to the algebra of quantics*. Second edn., Clarendon Press, Oxford, 1913. Zbl 44.0155.05

[4] J.-L. Lagrange, Réflexions sur la résolution algébrique des équations. Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin, années 1770 et 1771. In *Oeuvres complètes. Volume 3*, pp. 205–421, Gauthier-Villars, Paris, 1867.

(Reçu le 29 juin 2023)

Alain Connes, Collège de France, 3 rue d'Ulm, 75231 Paris, France;
e-mail: alain@connes.org

Jacques Dixmier, 11 bis rue du Val de Grâce, 75005 Paris, France