Théorème de Ruffini et Abel

On donne dans cette note une démonstration d'un résultat dû à Ruffini (1799) et Abel (1824) énoncant qu'on ne peut pas donner de formule générique pour exprimer les racines d'un polynôme quelconque de degré 5 à l'aide uniquement des opérations élémentaires d'addition, soustraction, multiplication, division et d'un nombre fini de racines $k^{\text{ième}}$ itérées. Ce résultat est à mettre en regard du fait que de telles formules existent pour les polynômes de degré $2, 3$ et 4. La démonstration que l'on présente est due à V.I. Arnold. (Elle n'est contenue à ma connaissance dans aucun livre sous une forme aussi concise.) Quelques notations sont nécessaires pour poser le décor et énoncer le résultat. Pour $z = re^{i\theta} \in \mathbb{C}\backslash\{0\}$, avec $\theta \in [0, 2\pi)$, et $k \in \mathbb{N}$, posons

$$z^{1/k} = r^{1/k} \exp\left(i\Big(\frac{\theta}{k} + \frac{2\pi p}{k}\Big)\right),$$

où $0 \leqslant p < k$ est entier. On utilisera de facon abusive la notation $z^{1/k}$ pour l'un de k nombres ci-dessus. On notera F une fonction d'un nombre fini de variables complexes qui s'exprime à l'aide des opérations élémentaires d'addition, soustraction, multiplication, division. Deux occurences du symbole F dans une même formule signalent des fonctions de ce type-là a priori différentes. On a par exemple, en notant $c = (c_0, c_1, c_2)$,

$$\frac{-c_1 + (c_1^2 - 4c_2c_0)^{1/2}}{2c_2} = F\big(c, F^{1/2}(c)\big). \tag{1}$$

On reconnait ici la formule donnant les racines d'un polynôme de degré 2. On notera F_1 une formule du type

$$F_1(c) = F\big(c, F^{1/k}(c)\big), \tag{2}$$

et, pour $n \geqslant 2$, on notera F_n une formule du type

$$F_n(c) = F\big(c, F_{n-1}^{1/k}(c)\big);$$

elle met en jeu au plus n racines $k^{\text{ième}}$ itérées et les opérations élémentaires sur ces quantités.[1]

Une remarque importante et déjà claire sur la définition de $z^{1/k}$. L'image d'un lacet par une application de type F_1 n'est pas forcément un lacet. Sur l'exemple de $z^{1/k}$, on suit continument les coordonnées polaire (θ_t, r_t) de $z(t)$ le long du chemin. Comparez le cas où le lacet $(z(t))_{0\leqslant t\leqslant 1}$ décrit un petit cercle au voisinage de z_0 au cas où le lacet décrit un certain nombre de tours complets autour du point 0. Le point $z(1)$ est l'image de $z(0)$ par une rotation d'angle $\theta_1 - \theta_0$. A fortiori, l'image d'un lacet par une application de type F_n peut ne pas être un lacet.

Théorème − *Quel que soit $n \geqslant 1$, il n'existe pas de formule de la forme*

$$s = F_n(c),$$

donnant l'ensemble $s \in \mathbb{C}^5$ des racines d'un polynôme quelconque sur $\mathbb{C}$ de degré 5, en terme de ses coefficients $c = (c_0, \ldots, c_5) \in \mathbb{C}^6$.

On prend comme point de départ le fait que chaque coefficient d'un polynôme est une fonctions symétrique élémentaires des racines s de ce polynôme, ce qu'on écrit $c = f_{\text{sym}}(s)$, où c désigne l'ensemble des coefficients. Si donc $(s(t))_{0\leqslant t\leqslant 1}$ désigne un chemin continu dans $\mathbb{C}^5$ tel que $s(1)$ est une permutation non triviale de $s(0)$ alors $c(t) := f_{\text{sym}}(s(t))$ décrit un lacet dans $\mathbb{C}^6$, du fait que la fonction f_{sym} est invariante par permutation de ses arguments. On va voir que pour un polynôme de degré (supérieur ou égal à) 5, de racines s, pour toute formule de type F_n on peut trouver un chemin $(s(t))_{0\leqslant t\leqslant 1}$ issu de s tel que $s(1)$ est une permutation non triviale de s, en particulier $s(1) \neq s(0)$, et tel que $F_n(c(1)) = F_n(c(0))$. Cela empêche d'avoir

[1] En d'autres termes, une formule de type F_1 peut contenir au plus une racine $k^{\text{ième}}$ et les opérations élémentaires sur ces quantités, comme dans $c_0^{1/2}$ ou $c_0^{1/2}(c_1 + c_2)^{1/3}$, une formule de type F_2 peut contenir au plus deux racines de type $k^{\text{ième}}$ itérées et les opérations élémentaires sur ces quantités„ comme dans $\big(c_0 + (c_1c_2)^{1/3}\big)^{1/2}$ ou $\big(c_0 + (c_1c_2)^{1/3}\big)^{1/2}\big(c_0 + (c_1c_2)^{1/4}\big)^{1/5}$, et une formule de type F_3 trois racines de type $k^{\text{ième}}$ itérées et les opérations élémentaires sur ces quantités„ comme dans $\big(c_0 + \big(c_1c_2 + (c_0)^{1/4}\big)^{1/3}\big)^{1/2}$.

l'identité $s = F_n(c)$, qui impliquerait la contradiction $s(1) = s(0)$, alors que $s(1) \neq s(0)$, du fait qu'un polynôme générique a des racines distinctes. Allons-y graduellement pour faire émerger le raisonnement.

• Une évidence, d'abord, qui met déjà en jeu le mécanisme fondamental. On ne peut pas décrire l'ensemble $s \in \mathbb{C}^2$ des racines d'un polynôme sur $\mathbb{C}$ de degré 2, de coefficients $c = (c_0, c_1, c_2) \in \mathbb{C}^3$, à l'aide d'une formule du type F, i.e. comme une fraction rationnelle des coefficients. Notons (s_1, s_2) le couple ordonné des racines d'un polynôme de degré 2, *génériquement distinctes*, et rappelons qu'une formule de type F envoie un lacet sur un lacet. Si nous avions $s = F(c)$ et si $(s(t))_{0 \leqslant t \leqslant 1}$ désignait un chemin continu allant de (s_1, s_2) à (s_2, s_1), le chemin $c(t) = f_{\mathrm{sym}}(s(t))$ serait un lacet, et on aurait la contradiction

$$(s_1, s_2) = F\big(c\big) = F\big(c(0)\big) = F\big(c(1)\big) = (s_2, s_1).$$

On sait par contre qu'on peut écrire $s = F_1(c)$, à l'aide d'une racine $k^{\text{ième}}$, comme en (1).

• Considérons maintenant le cas des polynômes de degré 3, qui ont génériquement *trois racines distinctes* (s_1, s_2, s_3). Désignons par σ_{12} un chemin dans $\mathbb{C}^3$ envoyant (s_1, s_2, s_3) sur (s_2, s_1, s_3), et notons σ_{23} un chemin dans $\mathbb{C}^3$ envoyant (s_1, s_2, s_3) sur (s_1, s_3, s_2). Les chemins associés $\gamma_{ij} := f_{\mathrm{sym}} \circ \sigma_{ij}$ dans l'espace des coefficients $\{c\}$ sont par contre des lacets de $\mathbb{C}^4$, du fait que f_{sym} est invariante par permutation de ses arguments.. Je noterai $\gamma_{12} \star \gamma_{23}$ la concaténation des chemins consistant à d'abord suivre γ_{12} puis γ_{23}, et je noterai $(\gamma_{ij})^{-1}$ le chemin γ_{ij} parcouru en sens inverse.[2] Comme on l'a noté juste avant l'énoncé du théorème, et avec la notation (2) pour F_1, le point $F^{1/k}(\gamma_{12}(1))$ est obtenu à partir de $F^{1/k}(\gamma_{12}(0))$ par une rotation d'un certain angle, disons θ^1. Pareillement, le point $F^{1/k}(\gamma_{12} \star \gamma_{23}(1))$ est obtenu à partir de $F^{1/k}(\gamma_{12} \star \gamma_{23}(0))$ par une rotation d'un certain angle, disons θ^2. Il s'ensuit que $F^{1/k}$ envoie le lacet

$$\gamma := [\gamma_{12}, \gamma_{23}] := \gamma_{12} \star \gamma_{23} \star (\gamma_{12})^{-1} \star (\gamma_{23})^{-1}$$

sur un lacet (les quatre angles s'ajoutent !), et que F_2 fait de même. On parle de γ comme du *commutateur des chemins* γ_{12} *et* γ_{23}. Dans le même temps, le lacet

$$\sigma := [\sigma_{12}, \sigma_{23}] := \sigma_{12} \star \sigma_{23} \star (\sigma_{12})^{-1} \star (\sigma_{23})^{-1}$$

induit la permutation non triviale

$$\big[(12), (23)\big] := (12)(23)(12)^{-1}(23)^{-1} = (123)$$

sur l'ensemble des racines (s_1, s_2, s_3) du polynôme considéré, avec en particulier $\sigma(1) \neq \sigma(0)$. *Il n'est donc pas possible que* $s = F_1(c)$, sans quoi on aurait

$$\sigma(t) = F_1\big((f_{\mathrm{sym}} \circ \sigma)(t)\big) = F_1\big(\gamma(t)\big)$$

le long du chemin, et la contradiction

$$\begin{aligned} \sigma(0) = (s_1, s_2, s_3) = F_1(c) &= F_1\Big(\gamma_{12} \star \gamma_{23} \star (\gamma_{12})^{-1} \star (\gamma_{23})^{-1}(0)\Big) \\ &= F_1\Big(\gamma_{12} \star \gamma_{23} \star (\gamma_{12})^{-1} \star (\gamma_{23})^{-1}(1)\Big) = (s_2, s_3, s_1) = \sigma(1). \end{aligned}$$

On sait par contre qu'on peut écrire $s = F_2(c)$, à l'aide d'une racine $k^{\text{ième}}$ itérée une fois.

• Un polynôme de degré 4 a génériquement quatre *racines distinctes* $(s_1, \dots, s_4)$. Pour $i \neq j$ dans $\{1, \dots, 4\}$, notons σ_{ij} un chemin de $\mathbb{C}^4$ échangeant s_i et s_j et laissant les deux autres racines fixes. Pour i, j, k, ℓ tous distincts, le chemin

$$\sigma := \big[[\sigma_{ij}, \sigma_{jk}], [\sigma_{jk}, \sigma_{k\ell}]\big]$$

permute l'ensemble $\{s_1, \dots, s_4\}$ et y induit la permutation non triviale

$$\big[[(ij), (jk)], [(jk), (k\ell)]\big] = (i\ell)(jk).$$

---

[2] On paramètre tous nos chemins par l'intervalle $[0, 1]$. La paramétrisation des chemins n'a aucune importance ici.

Prenons $(i,j,k,\ell) = (1,2,3,4)$. L'image par $f_{\rm sym}$ du chemin σ dans l'espace $\mathbb{C}^5$ des coefficients de $\mathbb{C}_4[X]$ est le lacet

$$\gamma := \big[[\gamma_{12},\gamma_{23}],[\gamma_{23},\gamma_{34}]\big],$$

où $\gamma_{ij} = f_{\rm sym}\circ\sigma_{ij}$. Une fonction de type F_2 est de la forme

$$F_2(c) = F\Big(c, F^{1/k_1}\big(c, F^{1/k_2}(c)\big)\Big).$$

Chaque fonction $\Big([\gamma_{12},\gamma_{23}], F^{1/k_2}\big([\gamma_{12},\gamma_{23}]\big)\Big)$ et $\Big([\gamma_{23},\gamma_{34}], F^{1/k_2}\big([\gamma_{23},\gamma_{34}]\big)\Big)$ décrit un lacet d'après ce qu'on a vu au point précédent. L'image par $F^{1/k_1}\big(c, F^{1/k_2}(c)\big)$ du commutateur des deux lacets $[\gamma_{12},\gamma_{23}]$ et $[\gamma_{23},\gamma_{34}]$ produit donc un lacet, d'après l'analyse du point précédent; il en va de même pour F_2. *Il n'est donc pas possible que* $s = F_2(c)$, sans quoi on aurait

$$\sigma(t) = F_2\big((f_{\rm sym}\circ\sigma)(t)\big) = F_2\big(\gamma(t)\big)$$

le long du chemin, et la contradiction

$$(s_1,\dots,s_4) = \sigma(0) = F_2(c) = F_2\big(\gamma(0)\big) = F_2\big(\gamma(1)\big) = \sigma(1) = (s_3,s_4,s_1,s_2) \neq (s_1,\dots,s_4).$$

On sait par contre qu'on peut écrire $s = F_3(c)$, à l'aide d'une racine $k^{\text{ième}}$ itérée deux fois.

Démonstration – Un polynôme de degré 5 a génériquement cinq *racines distinctes* $(s_1,\dots,s_5)$. Définissons

$$\mathscr{F}_0 := \Big\{\text{3-cycles des permutations de } \{1,\dots,5\}\Big\}$$
$$\mathscr{F}_n := \Big\{[a,b] = aba^{-1}b^{-1};\, a,b\in\mathscr{F}_{n-1}\Big\},\quad n\geqslant 1.$$

La relation

$$[(ijk),(k\ell m)] = (jkm), \tag{3}$$

valable pour tout i,j,k,ℓ,m dans $\{1,\dots,5\}$, implique que chaque trois cycle appartient à tous les $\mathscr{F}_n$. Donnons-nous maintenant pour chaque $i\neq j\in\{1,\dots,5\}$ un chemin σ_{ij} de $\mathbb{C}^5$ échangeant s_i et s_j et laissant fixe les autres racines, et définissons les lacets $\gamma_{ij} := f_{\rm sym}\circ\sigma_{ij}$. Définissons aussi

$$\mathscr{C}_0 := \Big\{[\gamma_{ij},\gamma_{jk}]\,;\, i,j,k \text{ distincts}\Big\}$$
$$\mathscr{C}_n := \Big\{[\gamma_a,\gamma_b];\, \gamma_a,\gamma_b\in\mathscr{F}_{n-1}\Big\},\quad n\geqslant 1.$$

Une récurrence élémentaire montre que, pour $n\geqslant 4$, l'image par une application de type F_{n-2} d'un lacet γ de $\mathscr{C}_n$ est un lacet. Le cas $n=4$ est analysé dans le point précédant le début de la démonstration. Le point crucial est qu'un tel lacet est l'image par $f_{\rm sym}$ d'un chemin σ de $\mathbb{C}^5$ obtenu en composant un certain nombre de σ_{ij}, tel que $\sigma(1)$ induit, d'après l'identité

$$[(ij),(jk)] = (ijk),$$

et l'identité (3), une permutation non triviale de $\{s_1,\dots,s_5\}$. Il n'est donc pas possible que $s = F_{n-2}(c)$, sans quoi on aurait

$$\sigma(t) = F_{n-2}\big((f_{\rm sym}\circ\sigma)(t)\big) = F_{n-2}\big(\gamma(t)\big)$$

le long du chemin, et la contradiction

$$(s_1,\dots,s_5) = \sigma(0) = F_{n-2}(c) = F_{n-2}\big(\gamma(0)\big) = F_{n-2}\big(\gamma(1)\big) = \sigma(1) \neq (s_1,\dots,s_5).$$

▷

References

[1] V.B. Alekseev, *Abel's theorem in problems and solutions.* Kluwer Academic Publishers, (2004).

[2] L. Goldmakher, *Arnold's elementary proof of the insolvability of the quintic.* https://web.williams.edu/Mathematics/lg5/394/ArnoldQuintic.pdf.

[3] P. Ramond, *Abel-Ruffini's Theorem: Complex but Not Complicated!* arXiv:2011.05162, (2020).