

Démonstration de l'impossibilité de résoudre toutes les équations algébriques avec des radicaux.

par M. Wantzel, répétiteur à l'École polytechnique

I.

Abel a entrepris de démontrer qu'une équation algébrique quelconque de degré supérieur au quatrième n'est pas résoluble par radicaux¹. Quoique sa démonstration soit exacte au fond, elle est présentée sous une forme trop compliquée et tellement vague, qu'elle n'a pas été généralement admise. Plusieurs années auparavant, Ruffini, géomètre italien, avait traité la même question d'une manière beaucoup plus vague encore, et avec des développements insuffisants, quoiqu'il soit revenu plusieurs fois sur le même sujet. En méditant les travaux de ces deux géomètres et à l'aide des principes que nous avons posés précédemment², nous sommes arrivé à une forme de démonstration qui paraît assez claire et assez précise pour lever tous les doutes sur cette partie importante de la théorie des équations.

Il faut d'abord bien poser la question. Résoudre une équation par radicaux, c'est exprimer les racines au moyen des coefficients par une fonction radicale d'une espèce déterminée, ou, ce qui est la même chose, ramener la résolution de l'équation proposée à celle d'une série d'équations binômes, dont les seconds termes dépendent successivement des coefficients et des racines des équations précédentes.

La question ainsi posée présente trois points de vue fort différents, soit qu'il s'agisse de résoudre une équation générale quels que soient les coefficients, soit qu'on s'occupe d'une équation déterminée pour savoir si elle est résoluble ou non par radicaux, soit enfin qu'on veuille obtenir les racines d'une équation par des extractions de racine effectuées sur des quantités réelles.

Quant au dernier cas, nous avons fait voir dans le mémoire précité³ que même pour les équations du troisième degré on ne pouvait exprimer les racines de cette manière lorsqu'elles sont toutes réelles, on le peut toujours au contraire quand il y en a deux imaginaires. Nous reviendrons sur ce travail qui est demeuré inachevé. Le second cas est le plus difficile de tous : il paraît avoir été à peine entrevu par Abel et il n'a été attaqué avec quelque succès que dans un mémoire inédit de Galois, qui sera publié prochainement. Nous ne considérerons ici que le premier point de vue c'est aussi le seul qui ait été envisagé dans les mémoires d'Abel et de Ruffini.

II.

Il s'agit donc de démontrer seulement qu'on ne peut reproduire une racine d'une équation générale de degré supérieur au quatrième, en effectuant successivement un nombre limité d'opérations sur les coefficients ou sur des fonctions symétriques de toutes les racines. Puisque les coefficients sont

Référence : Wantzel, *Démonstration de l'impossibilité de résoudre toutes les équations algébriques avec des radicaux*, Nouvelles annales de mathématiques 1^{re} série, tome 4 (1845), p. 57-65.

Transcription en L^AT_EX : Denise Vella-Chemla, novembre 2025.

1. *Journal de Crelle*, tome 1, page 65 ; et *Bulletin de Ferussac*, tome VI.

2. *Nouvelles Annales*, tome 11, page 117.

3. Tome II, p. 125 de ce Recueil.

supposés quelconques, les racines sont tout à fait arbitraires, et la question se réduit à un principe de combinaison.

Soit $f(x) = 0$ l'équation proposée, et $x_1, x_2, \dots, x_m$ ses m racines. Supposons qu'on puisse exprimer la racine x , par une fonction radicale d'espèce quelconque. Comme les principes que nous avons établis sur les radicaux numériques et sur leur classification s'appliquent entièrement aux radicaux algébriques, la valeur de x , pourra se mettre sous la forme ⁴

$$A + u + Bu^2 + \dots + Mu^{n-1} \quad (1)$$

dans laquelle $u = \sqrt[n]{a}$ ou $u^n = a$; a est une fonction radicale d'espèce inférieure à celle de x , et $A, B, \dots, M$ peuvent être de même espèce, mais de degré moindre. On en déduira aussi que la valeur de x , est racine d'une équation irréductible du $n^{\text{ième}}$ degré, dont les coefficients sont des fonctions de même genre que $A, B, \dots, M$. Toutes les racines de cette équation, obtenues en remplaçant u par les diverses valeurs de $\sqrt[n]{a}$, devront par conséquent satisfaire à l'équation proposée; et, en désignant par $\alpha, \alpha^2, \alpha^3, \dots$ les racines $n^{\text{ièmes}}$ de l'unité, on aura n relations de la forme :

$$\begin{aligned} x_1 &= A + u + Bu^2 + \dots + Mu^{n-1}, \\ x_2 &= A + \alpha u + B\alpha^2 u^2 + \dots + M\alpha^{n-1} u^{n-1}, \\ x_3 &= A + \alpha^2 u + B\alpha^4 u^2 + \dots + M\alpha^{2n-2} u^{n-1}, \text{ etc.} \end{aligned}$$

Si l'on ajoute ces égalités membre à membre, il vient

$$x_1 + x_2 + x_3 + \dots = nA;$$

si on les ajoute encore après avoir multiplié respectivement par $\alpha^n, \alpha^{n-1}, \alpha^{n-2}, \dots$ on obtient :

$$x_1 + \alpha^{n-1} x_2 + \alpha^{n-2} x_3 + \dots = un;$$

en multipliant par $\alpha^n, \alpha^{n-2}, \alpha^{n-4}$, on trouvera de même :

$$x_1 + \alpha^{n-2} x_2 + \alpha^{n-4} x_3 + \dots = nBu^2;$$

et ainsi de suite. Ces résultats proviennent de deux propriétés des racines $\alpha, \alpha^2, \dots, \alpha^n$ de l'unité : leur somme est égale à zéro et elles se reproduisent toutes par les puissances de chacune d'entre elles (excepté α^n ou 1), lorsque n est un nombre premier.

Ainsi les quantités $u, A, B, \dots, M$ et a qui entrent dans l'expression de x , sont égales à des fonctions rationnelles de plusieurs racines de l'équation proposée.

Considérons maintenant une des quantités $A, B, \dots, M$ et a , on pourra former une équation ayant pour racines les diverses valeurs de la fonction rationnelle qui la représente, au moyen des coefficients de l'équation $f(x) = 0$. Car soit, par exemple, $B = \varphi(x_1, x_2, x_3, \dots)$; le produit

$$[B - \varphi(x_1, x_2, x_3, \dots)][B\varphi(x_2, x_1, x_3, \dots)][B - \varphi(x_1, x_3, x_2, \dots)] \dots$$

4. Tome II, p. 125 de ce Recueil.

obtenu en disposant les racines $x_1, x_2, x_3, \dots, x_m$ de toutes les manières possible sera une fonction symétrique de toutes ces racines; en sorte que B sera donné par une équation $F(B) = 0$ de même forme que la proposée.

Si l'on ordonne la quantité B par rapport à l'un des radicaux de plus haute espèce qu'elle renferme, on aura une expression semblable à celle de x ,

$$B = A' + \nu + B'\nu^2 + \dots + M'\nu^{p-1}, \quad \text{avec } \nu^p = b,$$

d'où l'on déduira par le même raisonnement que les quantités $\nu, A', B', \dots, M'$ et b sont fonctions rationnelles des racines de l'équation $F(B) = 0$, et que par conséquent elles s'expriment aussi rationnellement en fonction des racines de l'équation proposée.

En opérant de même sur chacune des quantités $A', B', \dots, M'$ et b , on arriverait à la même conclusion, relativement aux quantités radicales dont elles dépendent; et, ainsi de suite, jusqu'aux derniers radicaux qui portent sur des expressions rationnelles par rapport aux coefficients de l'équation $f(x) = 0$.

Donc si une équation est résoluble par radicaux, chaque radical simple ou composé qui entre dans la valeur de l'inconnue est égal à une fonction rationnelle des racines de cette équation.

Les fonctions rationnelles des racines qui représentent les divers radicaux peuvent renfermer toutes ces racines ou seulement un certain nombre; il est toujours permis de les supposer entières⁵ pour en concevoir plus facilement les combinaisons.

Il est à remarquer que la démonstration précédente s'applique quel que soit le point de vue sous lequel on envisage la question de la résolution par radicaux.

III.

Étudions maintenant les propriétés de ces fonctions rationnelles des racines qui sont égales aux différents radicaux contenus dans la valeur (1) de x_1 . Si l'équation $f(x) = 0$ est satisfaite par cette valeur, quels que soient ses coefficients, on doit reproduire identiquement x_1 , en substituant dans (1) la fonction rationnelle correspondante à chaque radical, puisque les racines de l'équation sont alors entièrement arbitraires. De même, toute relation entre les racines devra être identique et ne cessera pas d'exister, si l'on y remplace ces racines les unes par les autres d'une manière quelconque.

Désignons par y le premier radical qui entre dans la valeur de x_1 , en suivant l'ordre du calcul, et soit $y^n = p$; p dépendra immédiatement des coefficients de $f(x) = 0$, et pourra s'exprimer par une fonction symétrique des racines $F(x_1, x_2, x_3, \dots)$; y sera une fonction rationnelle $\varphi(x_1, x_2, x_3, \dots)$

5. Toute fonction fractionnaire d'une racine de l'équation $f(x) = 0$ peut être remplacée par une fonction entière de cette racine. En effet, si l'on multiplie les deux termes de $\frac{F(x_1)}{\varphi(x_1)}$ par $\varphi(x_2)\varphi(x_3)\dots$, le dénominateur deviendra une fonction symétrique K ; quant au numérateur $F(x_2) \times \frac{K}{\varphi(x_1)}$, il sera une fonction entière de x_1 , puisque $\varphi(x_1), \varphi(x_2), \dots$ sont racines d'une certaine équation $\varphi^m + A\varphi^{m-1} + \dots + H\varphi + K = 0$, d'où l'on tire $\frac{K}{\varphi} - \varphi^{m-1} + A\varphi^{m-2} + \dots + H$. La même démonstration s'applique à une fonction de plusieurs racines.

des mêmes racines.

Comme la fonction φ n'est pas symétrique, sans quoi la racine $n^{\text{ième}}$ de p s'extrairait exactement, elle doit changer lorsqu'on permute deux racines : x_1, x_2 , par exemple ; mais la relation $\varphi^n = F$ sera toujours satisfaite. D'ailleurs la fonction F étant invariable par cette permutation, les valeurs de φ sont des racines de l'équation $y^n = p$, et l'on a :

$$\varphi(x_2, x_1, x_3, \dots) = \alpha \varphi(x_1, x_2, x_3, \dots) ;$$

si l'on remplace de part et d'autre x_1 par x_2 , et réciproquement, il vient :

$$\varphi(x_1, x_2, x_3, \dots) = \alpha \varphi(x_2, x_1, x_3, \dots) ;$$

d'où, en multipliant par ordre : $\alpha^2 = 1$.

Ce résultat prouve que le nombre n , supposé premier, est nécessairement égal à 2. Donc, *le premier radical qui se présente dans la valeur de l'inconnue, doit être du second degré*. C'est ce qui arrive en effet pour les équations qu'on sait résoudre.

Si dans la fonction φ , on effectue une permutation de trois lettres, en remplaçant x_1, x_2, x_3 , respectivement par x_2, x_3, x_1 , elle ne changera pas de valeur. En effet, on aura d'abord :

$$\varphi(x_2, x_3, x_1, x_4, \dots) = \alpha \varphi(x_1, x_2, x_3, x_4, \dots) ;$$

puis en répétant des deux côtés la même substitution :

$$\varphi(x_3, x_1, x_2, x_4, \dots) = \alpha \varphi(x_2, x_3, x_1, x_4, \dots),$$

et

$$\varphi(x_1, x_2, x_3, x_4, \dots) = \alpha \varphi(x_3, x_1, x_2, x_4, \dots),$$

d'où, en multipliant, $\alpha^3 = 1$; comme d'ailleurs α est une racine carrée de l'unité, il faut que α soit égal à 1, ou que les valeurs de φ soient égales.

On verrait de même que φ est invariable par les permutations de cinq lettres ou d'un nombre premier quelconque. Dans ces permutations on suppose qu'aucune lettre du groupe considéré ne conserve la même place c'est ce qu'on appelle, d'après M. Cauchy, des permutations circulaires de 3, 5, ... lettres.

Continuons la série des opérations indiquées par la valeur (1) de x_1 .

On combinera le premier radical avec les coefficients de $f(x) = 0$, ou la fonction φ avec des fonctions symétriques des racines, à l'aide des premières opérations de l'algèbre, et l'on obtiendra toujours une fonction des racines invariable par les permutations de trois lettres. Les radicaux subséquents pourront donner encore des fonctions du même genre, s'ils sont du second degré. Supposons qu'on soit arrivé à un radical, pour lequel la fonction rationnelle équivalente ne soit pas invariable par ces permutations. Désignons-le toujours par $y = \varphi(x_1, x_2, x_3, \dots)$; dans l'équation $y^n = p$, nous ferons encore $p = F(x_1, x_2, x_3, \dots)$; cette fonction ne sera plus symétrique, mais seulement invariable par

les permutations de trois lettres. Si l'on remplace x_1, x_2, x_3 par x_2, x_3, x_1 dans φ , la relation $\varphi^n = F$ subsistera toujours, et, puisque F ne change pas par cette substitution, il viendra :

$$\varphi(x_2, x_3, x_1, x_4, \dots) = \alpha \varphi(x_1, x_2, x_3, x_4, \dots) ;$$

d'où l'on conclura, comme ci-dessus, $\alpha^3 = 1$. Ainsi n sera égal à 3.

Si le nombre des quantités $x_1, x_2, x_3, \dots$ est supérieur à quatre, ou si l'équation $f(x) = 0$ est d'un degré plus élevé que le quatrième, on pourra effectuer dans φ une permutation circulaire de cinq lettres, en remplaçant x_1, x_2, x_3, x_4, x_5 , par x_2, x_3, x_4, x_5, x_1 ; la fonction F ne changera pas, et l'on aura :

$$\varphi(x_2, x_3, x_4, x_5, x_1, \dots) = \alpha \varphi(x_1, x_2, x_3, x_4, x_5, \dots) ;$$

puis en répétant de part et d'autre la même substitution :

$$\varphi(x_3, x_4, x_5, x_1, x_2, \dots) = \alpha \varphi(x_2, x_3, x_4, x_5, x_1, \dots) \text{ etc.}$$

Par la multiplication, on obtient $\alpha^5 = 1$; ce qui entraîne $\alpha = 1$, puisque α est une racine cubique de l'unité. Ainsi, la fonction φ est invariable par les permutations de cinq lettres. D'ailleurs elle ne changerait pas davantage, si l'on remplaçait x_3, x_2, x_5, x_1, x_4 par x_2, x_5, x_1, x_4, x_3 ; en sorte que l'on a :

$$\varphi(x_3, x_4, x_5, x_1, x_2, \dots) = \varphi(x_2, x_3, x_1, x_4, x_5, \dots) ;$$

mais on avait déjà :

$$\varphi(x_1, x_2, x_3, x_4, x_5, \dots) = \varphi(x_3, x_4, x_5, x_1, x_2, \dots) ;$$

donc

$$\varphi(x_2, x_3, x_1, x_4, x_5, \dots) = \varphi(x_1, x_2, x_3, x_4, x_5, \dots) ;$$

C'est-à-dire que la fonction φ doit être invariable par les permutations de trois lettres.

Ainsi tous les radicaux renfermés dans la racine d'une équation générale du degré supérieur au quatrième devraient être des fonctions rationnelles invariables par les permutations de trois racines. En substituant ces fonctions dans l'expression (1), on arrive à une égalité de la forme :

$$x_1 = \varphi(x_1, x_2, x_3, x_4, x_5, \dots)$$

qui doit être identique ce qui est impossible, puisque le second membre reste invariable quand on remplace x_1, x_2, x_3 par x_2, x_3, x_1 tandis que le premier change évidemment.

Donc, il est impossible de résoudre par radicaux, une équation générale du cinquième degré ou de degré supérieur.

La démonstration précédente fait voir en même temps que pour les équations du troisième et du quatrième degré, le premier radical, dans l'ordre des opérations, doit être un radical carré, et le second un radical cubique ; ces circonstances se présentent en effet dans les formules données par Lagrange et les autres géomètres.

Les résultats que nous venons d'indiquer seront aperçus avec plus de facilité, si nous ajoutons une propriété remarquable des fonctions rationnelles considérées ci-dessus : c'est que toute fonction

invariable par les permutations de trois lettres ne peut avoir plus de deux valeurs. D'abord une fonction de ce genre est invariable par les permutations de cinq lettres ; car si

$$\varphi(x_2, x_3, x_1, x_4, x_5, \dots) = \varphi(x_1, x_2, x_3, x_4, x_5, \dots),$$

on aura aussi en remplaçant x_1, x_4, x_3 par x_4, x_5, x_1

$$\varphi(x_2, x_3, x_4, x_5, x_1, \dots) = \varphi(x_1, x_2, x_3, x_4, x_5, \dots),$$

On verrait de même que la fonction φ ne change pas par les permutations de 7, 9... lettres. Les diverses valeurs de cette fonction s'obtiendront par conséquent en permutant deux lettres, puis deux autres lettres et ainsi de suite. Supposons que $\varphi(x_2, x_1, x_3, x_5, \dots)$ et $\varphi(x_1, x_2, x_3, x_4, \dots)$ soient deux valeurs différentes, je dis que toute permutation de deux lettres $\varphi(x_1, x_2, x_4, x_3, \dots)$ reproduira l'une de ces valeurs. En effet, il vient en remplaçant x_1, x_2, x_4 par x_2, x_4, x_1 : $\varphi(x_2, x_4, x_1, x_3, \dots) = \varphi(x_1, x_2, x_4, x_3, \dots)$, tandis que l'on trouve $\varphi(x_2, x_1, x_3, x_4, \dots) = \varphi(x_2, x_4, x_1, x_3, \dots)$, par la substitution de x_1, x_3, x_4 au lieu de x_4, x_1, x_3 ; d'où l'on conclura $\varphi(x_1, x_2, x_4, x_3, \dots) = \varphi(x_2, x_1, x_3, x_4, \dots)$.