# *Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas ;*

PAR M. L. WANTZEL,
Élève-Ingénieur des Ponts-et-Chaussées.

## I.

Supposons qu'un problème de Géométrie puisse être résolu par des intersections de lignes droites et de circonférences de cercle : si l'on joint les points ainsi obtenus avec les centres des cercles et avec les points qui déterminent les droites on formera un enchaînement de triangles rectilignes dont les éléments pourront être calculés par les formules de la Trigonométrie ; d'ailleurs ces formules sont des équations algébriques qui ne renferment les côtés et les lignes trigonométriques des angles qu'au premier et au second degré ; ainsi l'inconnue principale du problème s'obtiendra par la résolution d'une série d'équations du second degré dont les coefficients seront fonctions rationnelles des données de la question et des racines des équations précédentes. D'après cela, pour reconnaître si la construction d'un problème de Géométrie peut s'effectuer avec la règle et le compas, il faut chercher s'il est possible de faire dépendre les racines de l'équation à laquelle il conduit de celles d'un système d'équations du second degré composées comme on vient de l'indiquer. Nous traiterons seulement ici le cas où l'équation du problème est algébrique.

## II.

Considérons la suite d'équations :

$$(A)\begin{cases} x_1^2+Ax_1+B=0, & x_2^2+A_1x_2+B_1=0\ldots x_{n-1}^2+A_{n-2}x_{n-1}+B_{n-2}=0, \\ & x_n^2+A_{n-1}x_n+B_{n-1}=0, \end{cases}$$

dans lesquelles A et B représentent des fonctions rationnelles des quantités données $p$, $q$, $r\ldots$ ; $A_1$ et $B_1$ des fonctions rationnelles de $x_1$, $p$, $q$, $\ldots$ ; et, en général, $A_m$ et $B_m$ des fonctions rationnelles de $x_m$, $x_{m-1}, \ldots x_1$, $p$, $q\ldots$.

Toute fonction rationnelle de $x_m$ telle que $A_m$ ou $B_m$, prend la forme $\frac{C_{m-1}x_m + D_{m-1}}{E_{m-1}x_m + F_{m-1}}$ si l'on élimine les puissances de $x_m$ supérieures à la pre-

mière au moyen de l'équation $x_m^2+a_{m-1}x_m+B_{m-1}=0$, en désignant par $C_{m-1}$, $D_{m-1}$, $E_{m-1}$, $F_{m-1}$, des fonctions rationnelles de $x_{m-1},\ldots x_1$, $p$, $q\ldots$; elle se ramènera ensuite à la forme $A'_{m-1}x_m+B'_{m-1}$ en multipliant les deux termes de $\frac{C_{m-1}x_m+D_{m-1}}{E_{m-1}x_m+F_{m-1}}$ par $-E_{m-1}(A_{m-1}+D_m)+F_{m-1}$.

Multiplions l'une par l'autre les deux valeurs que prend le premier membre de la dernière des équations (A) lorsqu'on met successivement à la place de $x_{n-1}$ dans $A_{n-1}$ et $B_{n-1}$ les deux racines de l'équation précédente : nous aurons un polynome du quatrième degré en $x_n$ dont les coefficients s'exprimeront en fonction rationnelle de $x_{n-2}\ldots x_1$, $p$, $q,\ldots$; remplaçons de même successivement dans ce polynome $x_{n-2}$ par les deux racines de l'équation correspondante, nous obtiendrons deux résultats dont le produit sera un polynome en $x_n$ de degré $2^2$, à coefficient rationnel par rapport à $x_{n-3}\ldots x_1$, $p$, $q\ldots$; et, en continuant de la même manière, nous arriverons à un polynome en $x_n$ de degré $2^n$ dont les coefficients seront des fonctions rationnelles de $p$, $q$, $r\ldots$. Ce polynome égalé à zéro donnera l'équation finale $f(x_n)=0$ ou $f(x)=0$, qui renferme toutes les solutions de la question. On peut toujours supposer qu'avant de faire le calcul on a réduit les équations (A) au plus petit nombre possible. Alors une quelconque d'entre elles $x_{m+1}^2+A_mx_{m+1}+B_m=0$, ne peut pas être satisfaite par une fonction rationnelle des quantités données et des racines des équations précédentes. Car, s'il en était ainsi, le résultat de la substitution serait une fonction rationnelle de $x_m,\ldots x_1$, $p$, $q\ldots$ qu'on peut mettre sous la forme $A'_{m-1}x_m+B'_{m-1}$ et l'on aurait $A'_{m-1}x_m+B'_{m-1}=0$; on tirerait de cette relation une valeur rationnelle de $x_m$ qui substituée dans l'équation du second degré en $x_m$ conduirait à un résultat de la forme $A'_{m-2}x_{m-1}+B'_{m-2}=0$. En continuant ainsi, on arriverait à $A'x_1+B'=0$, c'est-à-dire que l'équation $x_1^2+Ax_1+B=0$ aurait pour racines des fonctions rationnelles de $p$, $q\ldots$; le système des équations (A) pourrait donc être remplacé par deux systèmes de $n-1$ équations du second degré, indépendants l'un de l'autre, ce qui est contre la supposition. Si l'une des relations intermédiaires $A'_{m-2}x_{m-1}+B'_{m-2}=0$, par exemple, était satisfaite identiquement, les deux racines de l'équation $x_{m-1}^2+A_{m-1}x_m+B_{m-1}=0$ seraient des fonctions rationnelles de $x_{m-1},\ldots x_1$, pour toutes les valeurs que peuvent prendre ces quantités, en sorte qu'on pourrait supprimer l'équation en $x_m$ et remplacer la racine successivement par ses deux valeurs dans les équations sui-

vantes, ce qui ramènerait encore le système des équations (A) à deux systèmes de $n-1$ équations.

## III.

Cela posé, l'*équation du degré* $2^n$, $f(x)=0$, *qui donne toutes les solutions d'un problème susceptible d'être résolu au moyen de n équations du second degré, est nécessairement irréductible*, c'est-à-dire qu'elle ne peut avoir de racines communes avec une équation de degré moindre dont les coefficients soient des fonctions rationnelles des données $p$, $q$....

En effet, supposons qu'une équation $F(x)=0$, à coefficients rationnels soit satisfaite par une racine de l'équation $x_n^2+A_{n-1}x_n+B_{n-1}=0$, en attribuant certaines valeurs convenables aux quantités $x_{n-1}$, $x_{n-2}\ldots x_1$. La fonction rationnelle $F(x_n)$ d'une racine de cette dernière équation peut se ramener à la forme $A'_{n-1}x_n+B'_{n-1}$, en désignant toujours par $A'_{n-1}$ et $B'_{n-1}$ des fonctions rationnelles de $x_{n-1}\ldots x_1$, $p$, $q\ldots$; de même $A'_{n-1}$ et $B'_{n-1}$ peuvent prendre l'un et l'autre la forme $A'_{n-2}x_{n-1}+B'_{n-2}$, et ainsi de suite; on arrivera ainsi à $A'_1x_2+B'_1$ où $A'_1$ et $B'_1$ peuvent être mis sous la forme $A'x_1+B'$ dans laquelle $A'$ et $B'$ représentent des fonctions rationnelles des données $p$, $q$.... Puisque $F(x_n)=0$ pour une des valeurs de $x_n$, on aura $A'_{n-1}x_n+B'_{n-1}=0$, et il faudra que $A'_{n-1}$ et $B'_{n-1}$ soient nuls séparément, sans quoi l'équation $x_n^2+A_{n-1}x_n+B_{n-1}=0$ serait satisfaite pour la valeur $-\frac{B'_{n-1}}{A'_{n-1}}$ qui est une fonction rationnelle de.. $x_{n-1},\ldots x_1$, $p$, $q\ldots$, ce qui est impossible; de même, $A'_{n-1}$ et $B'_{n-1}$ étant nuls, $A'_{n-2}$ et $B'_{n-2}$ le seront aussi et ainsi de suite jusqu'à $A'$ et $B'$ qui seront nuls identiquement, puisqu'ils ne renferment que des quantités données. Mais alors $A'_1$ et $B'_1$, qui prennent également la forme $A'x_1+B'$ quand on met pour $x_1$ chacune des racines de l'équation $x_1^2+Ax_1+B=0$, s'annuleront pour ces deux valeurs de $x_1$; pareillement, les coefficients $A'_2$ et $B'_2$ peuvent être mis sous la forme $A'_1x_2+B'_1$ en prenant pour $x_2$ l'une ou l'autre des racines de l'équation $x_2^2+A_1x_2+B_1=0$, correspondantes à chacune des valeurs de $x_1$, et par conséquent ils s'annulleront pour les quatre valeurs de $x_2$ et pour les deux valeurs de $x_1$ qui résultent de la combinaison des deux premières équations (A). On démontrera de même que $A'_3$ et $B'_3$ seront nuls en mettant pour $x_3$ les $2^3$ valeurs tirées des trois premières équations (A) conjointement avec les valeurs correspondantes de $x_2$ et $x_1$;

et continuant de cette manière on conclura que $F(x_n)$ s'annulera pour les $2^n$ valeurs de $x_n$ auxquelles conduit le système de toutes les équations (A) ou pour les $2^n$ racines de $f(x)=0$. Ainsi une équation $F(x)=0$ à coefficients rationnels ne peut admettre une racine de $f(x)=0$ sans les admettre toutes; donc l'équation $f(x)=0$ est irréductible.

## IV.

Il résulte immédiatement du théorème précédent que tout problème qui conduit à une équation irréductible dont le degré n'est pas une puissance de 2, ne peut être résolu avec la ligne droite et le cercle. Ainsi *la duplication du cube*, qui dépend de l'équation $x^3-2a^3=0$ toujours irréductible, ne peut être obtenue par la Géométrie élémentaire. Le problème *des deux moyennes proportionnelles*, qui conduit à l'équation $x^3-a^2b=0$ est dans le même cas toutes les fois que le rapport de $b$ à $a$ n'est pas un cube. La *trisection de l'angle* dépend de l'équation $x^3-\frac{3}{4}x+\frac{1}{4}a=0$; cette équation est irréductible si elle n'a pas de racine qui soit une fonction rationnelle de $a$ et c'est ce qui arrive tant que $a$ reste algébrique; ainsi le problème ne peut être résolu en général avec la règle et le compas. Il nous semble qu'il n'avait pas encore été démontré rigoureusement que ces problèmes, si célèbres chez les anciens, ne fussent pas susceptibles d'une solution par les constructions géométriques auxquelles ils s'attachaient particulièrement.

La division de la circonférence en parties égales peut toujours se ramener à la résolution de l'équation $x^m-1=0$, dans laquelle $m$ est un nombre premier ou une puissance d'un nombre premier. Lorsque $m$ est premier, l'équation $\frac{x^m-1}{x-1}=0$ du degré $m-1$ est irréductible, comme M. Gauss l'a fait voir dans ses *Disquisitiones arithmeticæ*, section VII; ainsi la division ne peut être effectuée par des constructions géométriques que si $m-1=2^n$. Quand $m$ est de la forme $a^\alpha$, on peut prouver, en modifiant légèrement la démonstration de M. Gauss que l'équation de degré $(a-1)a^{\alpha-1}$, obtenue en égalant à zéro le quotient de $x^{a^\alpha}-1$ par $x^{a^{\alpha-1}}-1$, est irréductible; il faudrait donc que $(a-1)a^{\alpha-1}$ fût de la forme $2^n$ en même temps que $a-1$, ce qui est impossible à moins que $a=2$. Ainsi, *la division de la circonférence en* N *parties ne peut être effectuée avec la règle et le compas que si les facteurs premiers de* N *différents de* 2 *sont de la forme* $2^n+1$ *et s'ils entrent seulement à la première puissance dans ce nombre.* Ce

principe est annoncé par M. Gauss à la fin de son ouvrage, mais il n'en a pas donné la démonstration.

Si l'on pose $x = k + A' \sqrt[m']{a'} + A'' \sqrt[m'']{a''} + \text{etc.}$ $m', m'' \ldots$ étant des puissances de 2, et $k$, $A', A'' \ldots a', a'' \ldots$ des nombres commensurables, la valeur de $x$ se construira par la ligne droite et le cercle, en sorte que $x$ ne peut être racine d'une équation irréductible d'un degré $m$ qui ne soit pas une puissance de 2. Par exemple, on ne peut avoir, $x = A \sqrt[m]{a}$, si $(\sqrt[m]{a})^p$ est irrationnel pour $p < m$; on démontrerait facilement que $x$ ne peut prendre cette valeur lors même que $m$ serait une puissance de 2. Nous retrouvons ainsi plusieurs cas particuliers des théorèmes sur les nombres incommensurables que nous avons établis ailleurs (*).

## V.

Supposons qu'un problème ait conduit à une équation de degré $2^n$, $F(x)=0$ et qu'on se soit assuré que cette équation est irréductible; il s'agit de reconnaître si la solution peut s'obtenir au moyen d'une série d'équations du second degré.

Reprenons les équations (A) :

$$(A)\quad \begin{cases} x_1^2 + Ax_1 + B = 0, & x_2^2 + A_1 x_2 + B_1 = 0 \ldots, \\ x_{n-1}^2 + A_{n-2} x_{n-1} + B_{n-2} = 0, & x_n^2 + A_{n-1} x_n + B_{n-1} = 0. \end{cases}$$

Il faudra construire l'équation $f(x) = 0$, à coefficients rationnels, qui donne toutes les valeurs de $x_n$ et l'identifier avec l'équation donnée $F(x) = 0$. Pour faire ce calcul on remarque que $A_{n-1}$ et $B_{n-1}$ se ramènent à la forme $a_{n-1} x_{n-1} + a'_{n-1}$ et $b_{n-1} x_{n-1} + b'_{n-1}$, en sorte que l'élimination de $x_{n-1}$ entre les deux dernières équations (A) se fait immédiatement, ce qui donne une équation du quatrième degré en $x_n$; on y remplacera ensuite $a_{n-1}$ par $a''_{n-1} x_{n-2} + a'''_{n-1}$, $a'_{n-1}$ par $a^{IV}_{n-1} x_{n-2} + a^V$, $b_{n-1}$ par $b''_{n-1} x_{n-2} + b'''_{n-1}$, $b'_{n-1}$ par $b^{IV}_{n-1} x_{n-2} + b^V_{n-1}$ et $A_{n-2}$, $B_{n-1}$ par $a_{n-2} x_{n-2} + a'_{n-2}$, $b_{n-2} x_{n-2} + b'_{n-2}$, puis on éliminera $x_{n-2}$ entre l'équation du 4e degré déjà obtenue et l'équation $x_{n-2}^2 + A_{n-3} x_{n-2} + B_{n-3} = 0$; et ainsi de suite. Les derniers termes des séries $a_{n-1}$, $a'_{n-1}$, $a''_{n-1} \ldots$, $b_{n-1}$, $b'_{n-1} \ldots$, etc., doivent être des fonctions rationnelles des coefficients de $F(x) = 0$; si l'on peut leur assigner des valeurs rationnelles qui satisfassent aux équations de condition obtenues en identifiant, on reproduira les équations (A) dont le système équivaut à l'équation

(*) *Journal de l'École Polytechnique*, Cahier XXVI.

$F(x)=0$; si les conditions ne peuvent être vérifiées en donnant des valeurs rationnelles aux indéterminées introduites, le problème ne peut être ramené au second degré.

On peut simplifier ce procédé, en supposant que les racines de chacune des équations (A) donnent le dernier terme de la suivante; ainsi, l'on peut prendre $B_{n-1}$ pour l'inconnue de l'avant-dernière équation, puisque $B_{n-1}=b_{n-1}x_{n-1}+b'_{n-1}$ d'où $x_{n-1}=\frac{B_{n-1}-b'_{n-1}}{b_{n-1}}$; de cette manière les éliminations se font plus rapidement et l'on introduit quatre quantités indéterminées dans l'équation du quatrième degré qui résulte de la première élimination, huit dans l'équation du huitième degré, etc., en sorte que les conditions obtenues en identifiant sont en même nombre que les quantités à déterminer. Mais on écarte aussi à l'avance le cas où l'une des quantités telle que $b_{n-1}$ serait nulle, et il faut étudier ce cas séparément.

Soit, par exemple, l'équation $x^4+px^2+qx+r=0$. Prenons de suite les équations du second degré sous la forme $x_1^2+Ax_1+B=0$, et $x^2+(ax_1+a')x+x_1=0$; en éliminant $x_1$ et identifiant, on aura,

$$2a_1-Aa=0,\quad a'^2-Aaa'-A+a^2B=p,\quad 2aB-a'A=q,\quad B=r,$$

d'où

$$B=r,\quad a=\frac{2q}{4r-A^2},\quad a'=\frac{Aq}{4r-A^2},\quad A^3+pA^2-4rA+q^2-4rp=0.$$

Comme B, $a$ et $a'$ sont exprimés rationnellement au moyen de A, $p$, $q$, $r$, il faut et il suffit que l'équation du troisième degré en A ait pour racine une fonction rationnelle des données. La condition est toujours satisfaite quand $q=0$, quels que soient $p$ et $r$, car $A=-p$ satisfait alors à la dernière équation.

En prenant $x_1$ pour dernier terme de la deuxième équation du second degré, on a exclu le cas où ce terme serait indépendant de la racine de la première équation; mais en le traitant directement, on ne trouve aucune solution de la question qui ne soit comprise dans les équations ci-dessus.

Ainsi, par un calcul plus ou moins long, on pourra toujours s'assurer si un problème donné est susceptible d'être résolu au moyen d'une série d'équations du second degré, pourvu qu'on sache reconnaître si une équation peut être satisfaite par une fonction rationnelle des données, et si elle est irréductible. Une équation de degré $n$ sera irréductible lorsqu'en cherchant les diviseurs de son premier

membre de degrés $1, 2 \ldots \frac{n}{2}$, on n'en trouve aucun dont les coefficients soient fonctions rationnelles des quantités données.

La question peut donc toujours être ramenée à rechercher si une équation algébrique $F(x) = 0$ à une seule inconnue peut avoir pour racine une fonction de ce genre. Pour cela, il y a plusieurs cas à considérer. 1° Si les coefficients ne dépendent que de nombres donnés entiers ou fractionnaires, il suffira d'appliquer la méthode des racines commensurables. 2° Il peut arriver que les données représentées par les lettres $p, q, r$ soient susceptibles de prendre une infinité de valeurs, sans que la condition cesse d'être remplie, comme quand elles désignent plusieurs lignes prises arbitrairement; alors, après avoir ramené l'équation $F(x) = 0$ à une forme telle que ses coefficients soient des fractions entières de $p$, $q$, $r \ldots$, et que celui du premier terme soit l'unité, on remplacera $x$ par $a_m p^m - a_{m-1} p^{m-1} + \ldots + a_0$, et l'on égalera à zéro les coefficients des différentes puissances dans le résultat; les équations obtenues en $a^m$, $a_{m-1} \ldots$ seront traitées comme l'équation en $x$, c'est-à-dire qu'on y remplacera ces quantités par des fonctions entières de $q$, et ainsi de suite jusqu'à ce qu'ayant épuisé toutes les lettres on soit arrivé à des équations numériques qui rentreront dans le premier cas. 3° Lorsque les données sont des nombres irrationnels, ils doivent être racines d'équations algébriques qu'on peut supposer irréductibles; dans ce cas, si l'on remplace $x$ par $a_m p^m + \ldots + a_0$ dans $F(x) = 0$, le premier membre de l'équation en $p$, ainsi obtenue, devra être divisible par celui de l'équation irréductible dont le nombre $p$ est racine; en exprimant que cette division se fait exactement, on arrivera à des équations en $a_m$, $a_{m-1} \ldots$, que l'on traitera comme l'équation $F(x) = 0$, jusqu'à ce que l'on parvienne à des équations numériques. On doit remarquer que $m$ peut toujours être pris inférieur au degré de l'équation qui donne $p$.

Ces procédés sont d'une application pénible en général, mais on peut les simplifier et obtenir des résultats plus précis dans certains cas très étendus, que nous étudierons spécialement.