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 :

$$(\mathrm{A})\left\{\begin{array}{l} x_1^2+\mathrm{A}x_1+\mathrm{B}=0,\quad x_2^2+\mathrm{A}_1x_2+\mathrm{B}_1=0\ldots x_{n-1}^2+\mathrm{A}_{n-2}x_{n-1}+\mathrm{B}_{n-2}=0,\\ \qquad\qquad x_n^2+\mathrm{A}_{n-1}x_n+\mathrm{B}_{n-1}=0,\end{array}\right.$$

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 $\frac{\mathrm{C}_{m-1}x_m+\mathrm{D}_{m-1}}{\mathrm{E}_{m-1}x_m+\mathrm{F}_{m-1}}$ si l'on élimine les puissances de x_m supérieures à la première 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 2^3, 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 suivantes, 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 $p, q\ldots.$

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 $A'_{n-2}x_{n-1}+B'_{n-1}$, 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 $p, q\ldots.$ 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 $x^3 - a^2 b = 0$ 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^α, 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.

[...]

Errata

Page 362, lignes 1, 2, 3 en remont., *au lieu de* γ, *lisez* v

362, 6, au coefficient de u, ajoutez $-b^2(A^2+C^2)$

363, 12, *au lieu de* $-a_{1,2}(\ldots\ldots)$, *lisez* $-a_{3,2}(\ldots\ldots)$

363, 2, en remont., *au lieu de* $:v(L''\cos\phi\ldots\ldots):V$, *lisez* $:v,(L''\cos\phi\ldots):v$

364, 13, 14, 15, *au lieu de* EX, EY, EZ, *lisez* $E\int X, E\int Y, E\int Z$

364, 1, en remont., *au lieu de* $=-$, *lisez* $=+$

364, 2, en remont., *au lieu de* $-\sin\varphi\cos^2\varphi$, *lisez* $-\sin\varphi\cos\varphi$

365, 10, *effacez* $\frac{1}{p}$

365, 10 et 11, *au lieu de* $\int$, *lisez* $c^2\int$

367 1, *au lieu de* a_{m-1}, *lisez* A_{m-1}

367, 4, *au lieu de* D_m *lisez* x_m

368, 23, *au lieu de* A'_{-1}, *lisez* A'_{n-1}

372 14, *au lieu de* $-$ *lisez* $+$

372 16, *au lieu de* a^m, *lisez* a_m

428, 1, 4, 6, *au lieu de* D_m, *lisez* D_{m-1}

428, 1, 4, 6, 11, 12, *au lieu de* D_{m+1}, *lisez* D_0

428, 16, *après ces mots* et à $\frac{2f1}{\varrho}$, *ajoutez* donc auparavant elles étaient $< \frac{2f1}{\varrho}$

435, 7, *au lieu de* $(in-1)$, *lisez* $(n-1)$

437 et 438, *au lieu de* paramètre, *lisez partout* demi-paramètre

441 12, *au lieu de* $\frac{d^2V}{dx^2} \quad (V+b^2x\int_{r0}^{1} xV\,dx)$, *lisez*

$$\frac{d^2V}{dx^2}+r(V+b^2x\int_0^1 xV\,dx)$$

449, ligne dernière, *au lieu de* $V'+b^2x\int_0^1 xV'dx$, *lisez*

$$r'(V'+b^2x\int_0^1 xV'dx)$$

451, ligne 17, *au lieu de* $\frac{\Psi}{2}$, *lisez* $\frac{\Psi}{i^2}$

FIN DU DEUXIÈME VOLUME.