Research on the means of knowing whether a problem in geometry can be solved with ruler and compass*

by M. L. Wantzel†
Student Engineer,‡National School of Bridges and Roads

I.

Suppose that a problem in geometry can be solved by intersections of straight lines and circumferences of circles: If one combines the points thereby obtained with the centers of the circles and with the points that determine the lines, the result is a set of right triangles whose elements could be calculated by the formulas of trigonometry; moreover, these formulas are algebraic equations of the first or second degree; thus the principal unknown of the problem is found by solving a series of quadratic equations whose coefficients are rational functions of the data and of the roots of the preceding equations. Accordingly, to know if a geometric construction can be performed with ruler and compass, it is necessary to ask if the roots of the equation to which the construction leads can be made to depend on a system of quadratic equations derived as indicated above. Here we shall consider only the case where the equation of the problem is algebraic.

II.

Consider the following system of equations:

$$\begin{aligned} x_1^2 + \mathbf{A}x_1 + \mathbf{B} &= 0 \\ x_2^2 + \mathbf{A}_1 x_2 + \mathbf{B}_1 &= 0 \\ &\vdots \\ x_{n-1}^2 + \mathbf{A}_{n-2}x_{n-1} + \mathbf{B}_{n-2} &= 0 \\ x_n^2 + \mathbf{A}_{n-1}x_n + \mathbf{B}_{n-1} &= 0 \end{aligned} \tag{A}$$

*Original publication: *Journal de Mathématiques Pures et Appliquées, ou Recueil Mensuel de Mémoires sur les Diverses Parties des Mathématiques*; Publié par Joseph Liouville. Tome Deuxième, 1837, pp. 366–372. Available at http://sites.mathdoc.fr/JMPA/feuilleter.php?id=JMPA_1837_1_2. Translated from the French by Brian Hayes, October 2006; revised January 2017. Please send corrections to brian@bit-player.org.

†The author's full name was Pierre Laurent Wantzel, so why does the byline read "M. L. Wantzel"? The M. stands for Monsieur. The use of this honorific is somewhat irregular in the early volumes of the *Journal*. Other bylines take the form "M. Poisson" or "M. Lebesgue" (without an initial), but Joseph Liouville, who was the journal's editor as well as the author of several papers, styles himself "J. Liouville" (without an M.). Wantzel is the only author given both an M. and an initial. That the initial is "L" suggests that Wantzel may have gone by Laurent rather than Pierre.

‡The title "Student Engineer" (Élève-Ingénieur) corresponds roughly to the rank of Master of Science. When Wantzel's paper was published in 1837, he was 23. A year later he was appointed professor of analysis at the École Polytechnique, and in 1840 became Ingénieur Ordinaire.

in which $\mathbf{A}$ and $\mathbf{B}$ represent rational functions of certain given quantities p, q, r,..., while $\mathbf{A}_1$ and $\mathbf{B}_1$ are rational functions of x_1, p, q, r,...; and, in general, $\mathbf{A}_m$ and $\mathbf{B}_m$ are rational functions of x_m, x_{m-1},..., x_1, p, q,....

Any rational function of x_m, such as $\mathbf{A}_m$ or $\mathbf{B}_m$, takes the form

$$\frac{\mathbf{C}_{m-1}x_m + \mathbf{D}_{m-1}}{\mathbf{E}_{m-1}x_m + \mathbf{F}_{m-1}}$$

if one eliminates powers of x_m higher than the first by means of the equation[1] $x_m^2 + \mathbf{A}_{m-1}x_m + \mathbf{B}_{m-1} = 0$, where $\mathbf{C}_{m-1}$, $\mathbf{D}_{m-1}$, $\mathbf{E}_{m-1}$ and $\mathbf{F}_{m-1}$ designate the rational functions of x_{m-1},..., x_1, p, q,...; the expression can then be reduced to the form $\mathbf{A}'_{m-1}x_m + \mathbf{B}'_{m-1}$ by multiplying the two terms from $\frac{\mathbf{C}_{m-1}x_m+\mathbf{D}_{m-1}}{\mathbf{E}_{m-1}x_m+\mathbf{F}_{m-1}}$ by $-\mathbf{E}_{m-1}(\mathbf{A}_{m-1} + \mathbf{D}_m) + \mathbf{F}_{m-1}$.

Within the last equation of the system (A), the variable x_{n-1} occurs inside each of the coefficients $\mathbf{A}_{n-1}$ and $\mathbf{B}_{n-1}$. For each such occurrence of x_{n-1} we can substitute the two roots (first one then the other) of the preceding equation. The substitution produces two values for the first term of the final equation (that is, x_n^2); multiplying one of these values by the other yields a fourth-degree polynomial in x_n whose coefficients are expressed as a rational function of $x_{n-2}, \ldots, x_1, p, q, \ldots$. Within this polynomial we can make corresponding substitutions for the variable x_{n-2}, using the two roots of the previous equation; we obtain two results whose product is a polynomial in x_n of degree 2^3, with rational coefficients in $x_{n-3}, \ldots, x_1, p, q, \ldots$. Continuing in the same manner, we arrive at a polynomial in x_n of degree 2^n, where the coefficients are rational functions of $p, q, r, \ldots$. Setting this polynomial equal to zero yields the final equation $f(x_n) = 0$ or $f(x) = 0$, which contains all the solutions of the problem.[2]

One can always suppose that before beginning the calculation one has reduced the equations (A) to the smallest possible number. Then no one of those equations, say $x_{m+1}^2 + \mathbf{A}_m x_{m+1} + \mathbf{B}_m = 0$, can be satisfied by a rational function of the quantities given and the roots of the preceding equations. Because, if that were possible, the result of substitution would be a rational function of $x_m, \ldots, x_1, p, q, \ldots$, which one can put in the form $\mathbf{A}'_{m-1}x_m + \mathbf{B}'_{m-1}$, and one would have $\mathbf{A}'_{m-1}x_m + \mathbf{B}'_{m-1} = 0$. From this relation we could derive a rational value of x_m which, substituted into the equation quadratic in x_m, would lead to a result of the form $\mathbf{A}'_{m-2}x_{m-1} + \mathbf{B}'_{m-2} = 0$. Continuing, one would arrive at $\mathbf{A}'x_1 + \mathbf{B}' = 0$, or in other words the equation $x_1^2 + \mathbf{A}x_1 + \mathbf{B} = 0$, which would have as roots certain rational functions of $p, q, \ldots$; the system of equations (A) could thus be replaced by two systems of $n-1$ quadratic equations, independent of one another, which contradicts the assumption. If one of the intermediate relations, such as $\mathbf{A}'_{m-2}x_{m-1} + \mathbf{B}'_{m-2} = 0$, were satisfied exactly, the two roots of the equation $x_{m-1}^2 + \mathbf{A}_{m-1}x_m + \mathbf{B}_{m-1} = 0$ would be rational functions of $x_{m-1}, \ldots, x_1$ for all the values that these quantities can assume, so that one could remove the equation in x_m and successively replace the root by its two values in the following equations, which would again reduce the system of equations (A) to two systems of $n-1$ equations.

III.

In summary, *the equation of degree 2^n, $f(x) = 0$, which gives all the solutions of a problem capable of being solved by means of n quadratic equations, is necessarily irreducible,* that is to say,

[1] TRANSLATOR'S NOTE: In the printed text the second term of the equation is $a_{m-1}x_m$, which I believe is a printer's error for $\mathbf{A}_{m-1}x_m$.

[2] TRANSLATOR'S NOTE: In the preceding paragraph I struggled to find a translation that was faithful to the French text and that also made mathematical sense. I failed. The result may well misrepresent both the language *and* the mathematics.

it cannot have roots in common with an equation of lesser degree whose coefficients are rational functions of the givens $p, q, \ldots$.

Suppose, on the contrary, that an equation $\mathbf{F}(x) = 0$ with rational coefficients is satisfied by a root of the equation $x_n^2 + \mathbf{A}_{n-1}x_n + \mathbf{B}_{n-1} = 0$, by assigning whatever values are needed to the quantities $x_{n-1}, x_{n-2}, \ldots, x_1$. The rational function $\mathbf{F}(x_n)$ of a root of this last equation can be reduced to the form $\mathbf{A}'_{n-1}x_n + \mathbf{B}'_{n-1}$. As always, we indicate by $\mathbf{A}'_{n-1}$ and $\mathbf{B}'_{n-1}$ rational functions of $x_{n-1}, \ldots, x_1, p, q, \ldots$; in the same way $\mathbf{A}'_{n-1}$ and $\mathbf{B}'_{n-1}$ can respectively take the form $\mathbf{A}'_{n-2}x_{n-1} + \mathbf{B}'_{n-2}$, and so on; we arrive thus at $\mathbf{A}'_1x_2 + \mathbf{B}'_1$, where $\mathbf{A}'_1$ and $\mathbf{B}'_1$ can be put in the form $\mathbf{A}'x_1 + \mathbf{B}'$, and where $\mathbf{A}'$ and $\mathbf{B}'$ represent rational functions of the data $p, q, \ldots$.

Since $\mathbf{F}(x_n) = 0$ must be true for one of the values of x_n, there must be a case where $\mathbf{A}'_{n-1}x_n + \mathbf{B}'_{n-1} = 0$. Furthermore, $\mathbf{A}'_{n-1}$ and $\mathbf{B}'_{n-1}$ must be null separately, since otherwise the equation $x^2 + \mathbf{A}_{n-1}x_n + \mathbf{B}_{n-1} = 0$ would be satisfied by the value $-\frac{\mathbf{B}'_{n-1}}{\mathbf{A}'_{n-1}}$, which is a rational function of $x_{n-1}, \ldots, x_1, p, q, \ldots$—and that is impossible. In the same way, if $\mathbf{A}'_{n-1}$ and $\mathbf{B}'_{n-1}$ are zero, then $\mathbf{A}'_{n-2}$ and $\mathbf{B}'_{n-2}$ must be zero also, and so on until $\mathbf{A}'$ and $\mathbf{B}'$ which will be identically zero, since they contain only quantities given. But then $\mathbf{A}'_1$ and $\mathbf{B}'_1$, which also take the form $\mathbf{A}'x_1 + \mathbf{B}' = 0$ when one substitutes for x_1 each root of the equation $x_1^2 + \mathbf{A}x_1 + \mathbf{B} = 0$, are canceled for these two values of x_1; likewise, the coefficients $\mathbf{A}'_2$ and $\mathbf{B}'_2$ can be put in the form $\mathbf{A}'_1x_2 + \mathbf{B}'_1$ by allowing x_2 to take the value of one or the other of the roots of the equation $x_2^2 + \mathbf{A}_1x_2 + \mathbf{B}_1 = 0$, corresponding to each value of x_1, and consequently they cancel for the four values of x_2 and the two values of x_1 that come from the combination of the first two equations (A). By the same principle one can show that $\mathbf{A}'_3$ and $\mathbf{B}'_3$ are made equal to zero by assigning to x_3 the 2^3 values drawn from the first three equations (A), together with the corresponding values of x_2 and x_1. Continuing in this manner, it is seen that $\mathbf{F}(x_n)$ has a zero for each of the 2^n values of x_n in all the equations (A), or for the 2^n roots of $f(x) = 0$. Thus an equation $\mathbf{F}(x) = 0$ with rational coefficients cannot admit any one root of $f(x) = 0$ without admitting them all; hence the equation $f(x) = 0$ is irreducible.

IV.

It follows immediately from the preceeding theorem that all problems that lead to an irreducible equation whose degree is not a power of 2 cannot be solved with straight lines and circles. Hence the *duplication of the cube*, which depends on the equation $x^3 - 2a^3 = 0$, which is always irreducible, cannot be done by elementary geometry. The problem of finding *two mean proportional numbers*, which leads to the equation $x^3 - a^2b = 0$, is in the same class whenever the ratio of b to a is not a cube. The *trisection of the angle* depends on the equation $x^3 - \frac{3}{4}x + \frac{1}{4}a = 0$. This equation is irreducible if it has no root that is a rational function of a, and that is the case as long as a remains algebraic; thus the problem cannot be solved in general with ruler and compass. It seems to us that it has never before been demonstrated rigorously that these problems—so famous among the ancients—are not susceptible to solution by the geometric constructions to which they were so attached.

The division of a circle into equal parts can always be reduced to the solution of the equation $x^m - 1 = 0$, in which m is a prime number or a power of a prime. When m is prime, the equation $\frac{x^m-1}{x-1} = 0$ of degree $m-1$ is irreducible, as Gauss has made clear in his *Disquisitiones arithmeticae*, section VII; thus the division cannot be accomplished by geometric construction if $m - 1 = 2^n$. When m is of the form a^α, one can prove, by slightly modifying the demonstration of Gauss, that an equation of degree $(a-1)a^{\alpha-1}$, obtained by setting equal to zero the quotient of $x^{a^\alpha} - 1$ by $x^{a^{\alpha-1}} - 1$, is irreducible. Thus it is necessary that $(a-1)a^{\alpha-1}$ be of the form 2^n at the same time as

$a-1$, which is impossible unless $a=2$. Hence, *the division of the circle into N parts can be done with ruler and compass only if the prime factors of N different from 2 are of the form 2^n+1 and if they include only the first power of this number.* This rule was stated by Gauss at the end of his work, but he did not give the proof.

In the equation

$$x = k + \mathbf{A}' \sqrt[m']{a'} + \mathbf{A}'' \sqrt[m'']{a''} + \text{etc.},$$

where m', m'',... are powers of 2 and k, $\mathbf{A}'$, $\mathbf{A}''$,..., a', a'',... are commensurable numbers, the value of x is constructable with lines and circles, and so x cannot be a root of an irreducible equation whose degree m is not a power of 2. For example, one cannot have $x = \mathbf{A}\sqrt[m]{a}$ if $(\sqrt[m]{a})^p$ is irrational for $p<m$; it is easy to show that x can take this value only when m is a power of 2. We have found several particular cases of the theorems on incommensurable numbers, which we have presented elsewhere[3].

V.

Let us suppose that a problem has led us to an equation of degree 2^n, $\mathbf{F}(x)=0$, and that we can be sure this equation is irreducible; then the question is whether the solution can be obtained by means of a series of second-degree equations.

Turning again to the equations (A):

$$\begin{aligned} x_1^2 + \mathbf{A}x_1 + \mathbf{B} &= 0 \\ x_2^2 + \mathbf{A}_1 x_2 + \mathbf{B}_1 &= 0 \\ &\vdots \\ x_{n-1}^2 + \mathbf{A}_{n-2}x_{n-1} + \mathbf{B}_{n-2} &= 0 \\ x_n^2 + \mathbf{A}_{n-1}x_n + \mathbf{B}_{n-1} &= 0, \end{aligned} \tag{A}$$

we need to construct an equation $f(x)=0$ with rational coefficients that gives all the values of x_n and to identify it with the given equation $\mathbf{F}(x)=0$. To perform this calculation we note first that $\mathbf{A}_{n-1}$ and $\mathbf{B}_{n-1}$ reduce to the form $a_{n-1}x_{n-1}+a'_{n-1}$ and $b_{n-1}x_{n-1}+b'_{n-1}$, so that x_{n-1} can be immediately eliminated in the last two equations (A), which yields an equation of the fourth degree in x_n. There, we can then replace:[4]

a_{n-1}	by	$a''_{n-1}x_{n-2}+a'''_{n-1}$,
a'_{n-1}	by	$a^{\text{iv}}_{n-1}x_{n-2}+a^{\text{v}}$,
b_{n-1}	by	$b''_{n-1}x_{n-2}+b'''_{n-1}$,
b'_{n-1}	by	$b^{\text{iv}}_{n-1}x_{n-2}+b^{\text{v}}$,
$\mathbf{A}_{n-2}$	by	$a_{n-2}x_{n-2}+a'_{n-2}$, and
$\mathbf{B}_{n-2}$	by	$b_{n-2}x_{n-2}+b'_{n-2}$

and then eliminate x_{n-2} in the fourth-degree equation we have just obtained as well as in the equation $x_{n-2}^2+\mathbf{A}_{n-3}x_{n-2}+\mathbf{B}_{n-3}=0$, and so on. The last terms in the series a_{n-1}, a'_{n-1},

[3] Author's note: *Journal de l'École Polytechnique*, Cahier XXVI.

[4] Translator's note: In the French text the last of the six quantities listed is given as $\mathbf{B}_{n-1}$; I believe it should be $\mathbf{B}_{n-2}$.

a''_{n-1},..., b_{n-1}, b'_{n-1},..., etc., should be rational functions of the coefficients of $\mathbf{F}(x) = 0$. If one can assign them rational values that satisfy the equations under the constraints identified, then one will reproduce the equations (A) in the system equivalent to the equation $\mathbf{F}(x) = 0$; if the conditions cannot be satisfied in giving rational values to the variables we have introduced, then the problem cannot be reduced to the second degree.

This procedure can be simplified by supposing that the roots of each of the equations (A) give the last term of the next equation. Thus, one can take $\mathbf{B}_{n-1}$ as the unknown in the penultimate equation, since $\mathbf{B}_{n-1} = b_{n-1}x_{n-1} + b'_{n-1}$, whence $x_{n-1} = \frac{\mathbf{B}_{n-1} - b'_{n-1}}{b_{n-1}}$. In this way the eliminations are made more rapidly, introducing four unknown quantities into the fourth-degree equation that results from the first elimination, eight into the eighth-degree equation, and so on, in such a way that the constraints imposed are of the same number as the quantities to be determined. But we must also set aside for separate handling the case where one of the quantities such as b_{n-1} is zero.

An example is the equation $x^4 + px^2 + qx + r = 0$. Let us continue by taking quadratic equations of the form $x_1^2 + \mathbf{A}x_1 + \mathbf{B} = 0$ and $x^2 + (ax_1 + a')x + x_1 = 0$; on eliminating x_1 and substituting we have:

$$\begin{aligned} 2a_1 - \mathbf{A}a &= 0, \\ a'^2 - \mathbf{A}aa' - \mathbf{A} + a^2\mathbf{B} &= p, \\ 2a\mathbf{B} - a'\mathbf{A} &= q, \\ \mathbf{B} &= r, \end{aligned}$$

where

$$\begin{aligned} \mathbf{B} &= r, \\ a &= \frac{2q}{4r - a^2}, \\ a' &= \frac{\mathbf{A}q}{4r - \mathbf{A}^2}, \\ \mathbf{A}^3 + p\mathbf{A}^2 - 4r\mathbf{A} + q^2 - 4rp &= 0. \end{aligned}$$

Since $\mathbf{B}$, a and a' are expressed as rational values in terms of $\mathbf{A}$, p, q and r, it is necessary and sufficient that the cubic equation in $\mathbf{A}$ have for its root a rational function of the given data. This condition is always satisfied when $q = 0$, whatever the values of p and r, because $\mathbf{A} = -p$ then satisfies the last equation.

In taking x_1 as the last term of the second quadratic equation, we have excluded the case where this term is independent of the root of the first equation; but in treating this case directly one will never encounter a solution that is not already among those of the equations above.

Thus, by a calculation more or less long, we can always be certain of knowing if a given problem is capable of solution by means of a series of quadratic equations, provided that we can recognize whether or not an equation can be satisfied by a rational function of the data and if it is irreducible. An equation of degree n is irreducible when a search of the divisors of the first term of degree 1, 2,..., $\frac{n}{2}$, reveals that none of the coefficients are rational functions of the given quantities.

The question can therefore always be reduced to determining whether an algebraic equation $\mathbf{F}(x) = 0$ of a single variable can have for its root a function of this kind. For this, there are several cases to consider:

1. If the coefficients depend only on given numbers that are integers or fractions, it is sufficient to apply the methods of commensurable roots.

2. It can happen that the data represented by the letters p, q, r can take on infinitely many values without ever fulfilling the conditions for solving the problem, as when they designate several lines situated arbitrarily; then, after having reduced the equation $\mathbf{F}(x) = 0$ to a form in which the coefficients are ratios of p, q, r,..., and in which the coefficient of the first term is unity, we can replace x by[5] $a_m p^m + a_{m-1} p^{m-1} + \cdots + a_0$, and set equal to zero the coefficients of the various powers in the result. Now the equations in a^m, a^{m-1},..., are to be treated in the same way as the equation in x, that is to say, we replace these quantities by functions of q alone, and continue in this manner until we have eliminated all the letters and are left with numerical equations that can be handled as in the first case.

3. When the data are irrational numbers, they must be roots of algebraic equations, which we can assume to be irreducible. In this case, if we replace x by $a_m p^m + \cdots + a_0$ in $\mathbf{F}(x) = 0$, the first term of the equation thereby obtained should be divisible by that of the irreducible equation of which the number p is the root; when this division can be done exactly, we arrive at equations in a^m, a^{m-1},..., which we treat like the equation $\mathbf{F}(x) = 0$, until we reach purely numerical equations. It should be noted that m can always be chosen less than the degree of the equation that yields p.

These procedures are arduous to carry out in general, but we can simplify them and get more precise results in certain very common cases, which we shall study with particular attention.

[5] TRANSLATOR'S NOTE: In the French text the second term of this equation has a minus sign for reasons I do not understand; I have made all terms positive.