On the means of recognizing whether a geometric construction can be made with straightedge and compass

by M.L. Wantzel, engineering student of the School of Bridges and Roads

(literal translation from the French by J. Little)

I.

Suppose that a geometric construction problem can be solved by intersections of straight lines and circles. If one joins the points obtained in this way with the centers of the circles and with the points that determine the lines, one will form a sequence of triangles whose sides can be calculated by the formulas of trigonometry. These formulas are algebraic equations that contain the side lengths only to the first or the second degree. So the principal unknown of the problem will be obtained by solving a series of equations of the second degree whose coefficients are rational functions of the given information and of the roots of the preceding equations. Because of this, in order to recognize whether the construction in a geometry problem can be carried out with the straightedge and compass, it is necessary to determine whether it is possible to make the roots of the equation to which the construction leads depend on roots of a composite system of second order equations as we have just indicated. We will treat only the case where the equation of the problem is algebraic.

II.

Consider a sequence of equations:

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

in which the A, B represent rational functions of given quantities $p, q, r, \ldots$, A_1, B_1 represent rational functions of $x_1, p, q, r, \ldots$, and generally A_m, B_m represent rational functions of $x_m, x_{m-1}, \ldots, x, p, q, r, \ldots$. Every rational function of x_m, such as A_m or B_m takes the form

$$\frac{C_{m-1}x_m + D_{m-1}}{E_{m-1}x_m + F_{m-1}}$$

if one eliminates powers of x_m higher than the first by means of the equation $x_m^2 + A_{m-1}x_m + B_{m-1} = 0$, while designating by $C_{m-1}, D_{m-1}, E_{m-1}, F_{m-1}$ the resulting rational functions of $x_{m-1}, \ldots, x, p, q, r, \ldots$. This [i.e. the preceding rational function with numerator and denominator linear in x_m] can also be put into the form $A'_{m-1}x_m + B'_{m-1}$

by multiplying the numerator and the denominator in $\frac{C_{m-1}x_m+D_{m-1}}{E_{m-1}x_m+F_{m-1}}$ by $-E_{m-1}(A_{m-1}+D_m)+F_{m-1}$.

Let us multiply together the two values that the first term in the equations (A) takes when one substitutes successively in the place of x_{n-1} in A_{n-1}, B_{n-1} the two roots of the preceding equation. We will have a polynomial of degree 4 in x_n whose coefficients are expressed as rational functions in $x_{n-1}, \ldots, x, p, q, \ldots$. If we replace x_{n-2} in the same way successively in this polynomial by the two roots of the corresponding equation, we will obtain two results of which the product will be a polynomial in x_n of degree $8 = 2^3$, with coefficients rational in $x_{n-3}, \ldots, x, p, q, \ldots$. Continuing in the same way, we will arrive at a polynomial in x_s of degree 2^s whose coefficients will be rational functions of $p, q, r, \ldots$. Setting this polynomial equal to zero will give a final equation $f(x_n) = 0$ or $f(x) = 0$ which includes all the solutions of the question. One can always suppose that, before doing this calculation, one has reduced the system (A) to the smallest possible number of equations. (We claim that) an arbitrary element of the system (A), say $x_{m+1}^2 + A_m x_{m+1} + B_m = 0$ cannot be satisfied by any rational function of the given quantities and the the roots of the preceding equations. (Proof:) For if that were true, the result of the substitution would be a rational function of $x_m, \ldots, x, p, q, \ldots$ that could be put in the form $A'_{m-1}x_m + B'_{m-1}$ and one would have $A'_{m-1}x_m + B'_{m-1} = 0$. One would take from this equation a rational value for x_m, which substituted into the second degree equation for x_m would lead to a result of the form $A'_{m-2}x_{m-1} + B'_{m-2} = 0$. Continuing in the same way, one would arrive at $A'x_1 + B' = 0$, that is that the equation $x_1^2 + Ax_1 + B = 0$ would have solutions that were rational functions of $p, q, \ldots$. The system (A) could then be replaced by two systems of $n-1$ equations of the second degree, independent of each other, which is a contradiction. If one of the intermediate relations $A'_{m-2}x_{m-1} + B'_{m-2} = 0$, for instance, were identically satisfied, the two solutions of the equation $x_{m-1}^2 + A_m x_{m-1} + B_m = 0$ would be rational functions of $x_{m-1}, \ldots, x$ for all the values that these quantities could hold, in such a way that the one could suppress the equation in x_m and relace the root successively by the two values in the following equations. This would again lead the system (A) to two systems of $n-1$ equations.

III.

We claim:

Theorem. *The equation of degree 2^s, $f(x) = 0$, that gives all the solutions of a problem that can be solved by means of n equations of the second degree, is necessarily irreducible.*

That is to say that f cannot have any roots in common with an equation of smaller degree whose coefficients are rational functions in $p, q, \ldots$.

(Proof:) Suppose in fact that an equation $F(x) = 0$, with rational coefficients, is solved by a root of the equation $x_n^2 + A_{n-1}x_n + B_{n-1} = 0$, where we attribute suitable values to $x_{n-1}, \ldots, x_1$. The rational function $F(x_n)$ of the root of this last equation can be brought to the form $A'_{n-1}x_n + B'_{n-1}$, where A'_{n-1}, B'_{n-1} designate rational function sof $x_{n-1}, \ldots, x_1, p, q, \ldots$. In the same way, A'_{n-1} and B'_{n-1} can both be brought to the form $A'_{n-1}x_{n-1} + B'_{n-2}$, and so forth. One will arrive this way at $A'_1x_2 + B'_1$ where A'_1 and B'_1 can be put in the form $A'x + B'$ where A' and B' are rational functions of the givens

$p, q, \ldots$. Since $F(x_n) = 0$ for one of the values of x_n, one will have $A'_{n-1}x_n + B'_{n-1} = 0$ and it is necessarily true that A'_{n-1} and B'_{n-1} are zero separately. Otherwise, the equation $x_n^2 + A_{n-1}x_n + B_{n-1} = 0$ would be solved by $x_n = -\frac{B'_{n-1}}{A'_{n-1}}$, which is a rational function of $x_{n-1}, \ldots, x_1, p, q$. This is impossible, however. Similarly, since $A'_{n-1} = B'_{n-1} = 0$, the same must be true of A'_{n-2} and B'_{n-2}. And similarly, in turn all these expressions down to A'_1 and B'_1 which must be zero because they contain only the given quantities. But A'_1 and B'_1, which also take the form $A'x_1 + B'$ when one substitutes for x_1 each of the roots of the equation $x_1^2 + Ax_1 + B = 0$, will vanish for these two values of x_1. Similarly, the coefficients A'_2 and B'_2 can be put in the form $A'_1x_2 + B'_1$, taking for x_2 either one of the roots of the equation $x_2^2 + A_1x_2 + B_1 = 0$, corresponding to each of the values of x_1. And hence they will vanish for the four values of x_2 and the two values of x_1 that result from the combination of the first two equations in (A). One can show similarly that A'_3 and B'_3 will be zero when we substitute for x_3 any of the 8 values taken from the first three equations in (A), together with the corresponding values of x_2 and x_1. Continuing in this way, one will conclude that $F(x_n)$ will vanish for all 2^n values of x_n coming from the whole system (A), or for the 2^n solutions of $f(x) = 0$. Thus an equation $F(x) = 0$ with rational coefficients cannot admit one root of $f(x) = 0$ as a solution without having all the roots of that equation as solutions. Hence the equation $f(x) = 0$ is irreducible.

IV.

It results immediately from the preceding theorem that any problem that leads to an irreducible equation whose degree is not a power of 2 cannot be solved using only the straightedge and compass. Thus the *duplication of the cube*, which depends on the solution of the equation $x^3 - 2a^3 = 0$, always irreducible (translator's note: i.e. irreducible for all values of a) cannot be obtained by elementary geometry. The problem of the *two mean proportionals*, which leads to an equation $x^3 - a^2b = 0$, is in the same case whenever the ratio of b and a is not a cube. The *trisection of the angle* leads to the equation $x^3 - \frac{3}{4}x + \frac{1}{4}a = 0$. This equation is irreducible if it has no roots that are rational functions of a, and this is the case if a is algebraic. Thus the problem cannot be solved in general using straightedge and compass. It seems to us that it has not before been shown rigorously that these problems, so celebrated among the ancients, cannot be solved using the geometric constructions they were particularly attached to.

The division of the circumference of a circle into equal parts can always be reduced to the solution of the equation $x^m - 1 = 0$, in which m is prime or a power of a prime number. When m is prime, the equation $\frac{x^m-1}{x-1}$ is irreducible, as M. Gauss proved in his *Disquisitiones Arithmeticae*, section VII. Thus the division cannot be made by geometric constructions unless $m - 1 = 2^s$. When m is of the form a^α, one can show, by slightly modifying M. Gauss's proof that the dation of degree $(a-1)a^{\alpha-1}$, obtained by setting $\frac{x^{a^\alpha}-1}{x^{a^{\alpha-1}}-1}$ equal to zero is irreducible. So it would be necessary for $(a-1)a^{\alpha-1}$ to be of the form 2^s at the same time that $a-1$ had that form, which is impossible unless $a = 2$. Thus,

Theorem. *The division of the circumference of a circle into N (equal) parts can only be accomplished with straightedge and compass when the prime factors of N different from 2 are of the form $2^s + 1$, and if they enter only to the first power in this number.*

This principle is announced by M. Gauss at the end of his work, but he did not give a proof.

If one poses $x = k + A' \sqrt[m']{a'} + A'' \sqrt[m'']{a''} + \cdots$, where m', m'', etc. are powers of 2 and $k, A', A'', a', a'', \ldots$ are commensurable numbers, the value of x can be constructed with straight lines and circles, in such a way that x cannot be a root of an irreducible equation of degree m that is not a power of 2. For example, one cannot have $x = A \sqrt[m]{a}$ if $(\sqrt[m]{a})^p$ if $p < m$. One can show easily that x cannot take these values unless m is a power of 2. We find in this way many particular cases of the theorems that we have established elsewhere.(*) [footnote: (*) Journal de l'École Polytechnique, Cahier XXVI.]

V.

Let us suppose that a problem has led to an equation of degree 2^s, $F(x) = 0$ and that we are sure that this equation is irreducible. It is now a matter of recognizing whether the equation can be obtained by means of a series of equations of the second degree. Let us reconsider the equations (A):

$$(A) \qquad \begin{aligned} x_1^2 + Ax_1 + B &= 0 \\ x_2^2 + A_1 x_2 + B_1 &= 0 \\ &\vdots \\ x_n^2 + A_{n-1} x_n + B_{n-1} &= 0. \end{aligned}$$

It is necessary to construct the equation $f(x) = 0$ with rational coefficients that gives all the values of x_n and to show that it is the same as the given equation $F(x) = 0$. To make this calculation, one remarks that A_{n-1} and B_{n-1} can be taken to the form $a_{n-1}x_{n-1} + a'_{n-1}$ and $b_{n-1}x_{n-1} + b'_{n-1}$ in such a way that the elimination of x_{n-1} between the last two equations in (A) is immediate. This gives an equation of degree 4 in x_n. One will replace in that equation a_{n-1} by $a''_{n-1}x_{n-2} + a'''_{n-1}$, a'_{n-1} by $a^{iv}_{n-1}x_{n-2} + a^{v}_{n-1}$, b_{n-1} by $b''_{n-1}x_{n-2} + b'''_{n-1}$, and b'_{n-1} by $b^{iv}_{n-1}x_{n-2} + b^{v}_{n-1}$ and A_{n-2}, B_{n-2} by $a_{n-2}x_{n-2} + a'_{n-2}$, $b_{n-2}x_{n-2} + b'_{n-2}$. Next one eliminates x_{n-2} between the equation of degree 4 already obtained and the equation $x^2_{n-2} + A_{n-3}x_{n-2} + B_{n-3} = 0$, and similarly for the next equations. The last terms of the series $a_{n-1}, a'_{n-1}, a''_{n-1}, \ldots$ and $b_{n-1}, b'_{n-1}, b''_{n-1}, \ldots$ must be rational functions of the coefficients of $F(x) = 0$. If one can assign them rational values that satisfy the conditions obtained by identifying them [translator's note: I think this means: by setting $f(x)$ and $F(x)$ equal], one will reproduce the equations (A) of which the whole system is equivalent to $F(x) = 0$. If the conditions cannot be verified by giving rational values to the indeterminates introduced, the problem cannot be reduced to the second degree.

One can simplify this procedure. Supposing that the roots of each of the equations in (A) give the last term in the next one. Thus one can take B_{n-1} for the unknown in the next-to-last equation since $B_{n-1} = b_{n-1}x_{n-1} + b'_{n-1}$, and hence $x_{n-1} = \frac{B_{n-1} - b'_{n-1}}{b_{n-1}}$. In this way, the eliminations are done more rapidly and one introduces four undetermined quantities in the equation of degree 4 that results from the first elimination, eight in the

equation of degree 8, and so on, [together with] the conditions obtained in identifying [$f(x)$ and $F(x)$]. But one take away in advance the case where one of the quantities such as b_{n-1} is zero, and it is necessary to study this case separately.

Suppose, for example, that the equation [i.e. $F(x)$] is $x^4+px^2+qx+r=0$. Let us take next the equations of degree 2 in the form $x_1^2+Ax_1+B=0$, and $x^2+(ax_1+a')x+x_1=0$. In eliminating x_1 and identifying [i.e. setting the resulting equation in x equal to $F(x)$ above], one will have:

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

from which we get

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

Since B, a, a' are expressed rationally in terms of A, p, q, r, it is necessary and sufficient that the equation of degree 3 in A has a rational function of the givens as a root. This is always true if $q = 0$, since whatever p, r are, $A = -p$ satisfes this last equation.

In taking x_1 as the last term in the second equation of degree 2, one has excluded the case where this term is independent of the root of the first equation. But in treating that case directly, one finds no solution of the question which is not included in the equations above.

Thus, by a more or less long calculation, one will always be able to see whether a given problem is susceptible of being solved by means of a series of equations of degree 2, provided that one can recognize whether an equation can be solved by a rational function of the givens, and whether the equation is irreducible. An equation of degree n will be irreducible when in searching the divisors of its first term of degrees $1, 2, \ldots, \frac{n}{2}$, one finds no solutions whose coefficients are rational functions of the given quantities.

The question can thus always be reduced to determining whether equations $F(x) = 0$ in one variable have solutions of this kind. For that, there are several cases to consider. 1^o If the coefficients depend only on given numbers that are integers or fractions, it will suffice to apply the method of commensurable roots [translator's note: I think this means what we would call the "rational roots test" for polynomials.] 2^o It can happen that the givens represented by the letters p, q, r can take infinitely many values, while the conditions continue to hold, as for example, when they [come from] several lines chosen arbitrarily [in the corresponding geometric construction]. Then after having taken the equation $F(x) = 0$ to a form such that the coefficients are entire functions [i.e. polynomials] in $p, q, r, \ldots$, and such that the leading coefficient is 1 [i.e. "monic polynomials"], one will replace x by $a_m p^m + a_{m-1}p^{m-1} + \cdots + a_0$ [translator's note: an apparent typo corrected here], and one will set the coefficients of the various powers of p in the result equal to zero. The resulting equations in $a_m, a_{m-1}, \ldots$ [translator's note: another apparent typo fixed here] will be treated as equations in x. That is to say that in them, one will replace these quantities by entire functions of q, and so forth. Eventually, when all these letters have been exhausted, one will arrive at numerical equations, which will return us to the first case. 3^o When the givens are irrational numbers, they must be roots of algebraic equations and these can be

assumed to be irreducible. In this case, if one replaces x by $a_m p^m + \cdots + a_0$ in $F(x) = 0$, the first term in the equation in p so obtained must be divisible by the irreducible equation of which p is a root. In expressing that this division is exact [i.e. that the remainder on division is zero], one will arrive at equations in $a_m, a_{m-1}, \ldots$ that one will treat [as? like?] the equation $F(x) = 0$, until one comes to numerical equations. One must remark that m can be always be taken smaller than the degree of the equation that gives p.

These procedures are painful to carry out in general, but one can simplify them and obtain more precise results in some very extended cases that we will especially study [i.e. in detail].