93. From A Memoir on Algebraic Equations, Proving the Impossibility of a Solution of the General Equation of the Fifth Degree (1824)*

(Equations of higher degree than four cannot be solved by root extractions, except for special values of the coefficients)

NIELS ABEL

The mathematicians have been very much absorbed with finding the general solution of algebraic equations, and several of them have tried to prove the impossibility of it. However, if I am not mistaken, they have not as yet succeeded. I therefore dare hope that the mathematicians will receive this memoir with good will, for its purpose is to fill this gap in the theory of algebraic equations.

Let

$$y^5 - ay^4 + by^3 - cy^2 + dy - e = 0$$

be the general equation of fifth degree and suppose that it can be solved algebraically,—*i.e.*, that y can be expressed as a function of the quantities a, b, c, d, and e, composed of radicals. In this case, it is clear that y can be written in the form

$$y = p + p_1R^{\frac{1}{m}} + p_2R^{\frac{2}{m}} + \ldots + p_{m-1}R^{\frac{m-1}{m}},$$

m being a prime number, and R, p, p_1, p_2, etc. being functions of the same form as y. We can continue in this way until we reach rational functions of a, b, c, d, and e. We may also assume that $R^{\frac{1}{m}}$ cannot be expressed as a rational function of a, b, etc., p, p_1, p_2, etc., and substituting $\frac{R}{p_1^m}$ for R, it is obvious that we can make $p_1 = 1$.

Then

$$y = p + R^{\frac{1}{m}} + P_2R^{\frac{2}{m}} + \ldots + p_{m-1}R^{\frac{m-1}{m}}$$

Substituting this value of y in the proposed equation, we obtain, on reducing, a result in the form

$$P = q + q_1R^{\frac{1}{m}} + q_2R^{\frac{2}{m}} + \ldots + q_{m-1}R^{\frac{m-1}{m}} = 0,$$

q, q_1, q_2, etc. being integral rational functions of a, b, c, d, e, p, p_2, etc. and R.

For this equation to be satisfied, it is necessary that $q = 0$, $q_1 = 0$, $q_2 = 0, \ldots q_{m-1} = 0$. In fact, letting $z = R^{\frac{1}{m}}$, we have the two equations

$$z^m - R = 0, \text{ and } q + q_1z + \ldots + q_{m-1}z^{m-1} = 0.$$

If now the quantities q, q_1, etc. are not equal to zero, these equations must necessarily have one or more common roots. If k is the number of these roots, we know that we can find an equation of degree k, whose roots are the k roots mentioned, and whose coefficients are rational functions of R, q, q_1, and q_{m-1}. Let this equation be

$$r + r_1z + r_2z^2 + \ldots + r_kz^k = 0.$$

It has all its roots in common with the equation $z^m - R = 0$; now all the roots of this equation are of the form $\alpha_\mu z$, α_μ being one of the roots of the equation $\alpha_\mu{}^m - 1 = 0$. On substituting, we obtain the following equations

$$r + r_1z + r_2z^2 + \ldots + r_kz^k = 0,$$

$$r + \alpha r_1z + \alpha^2r_2z^2 + \ldots + \alpha^kr_kz^k = 0,$$

$$\ldots\ldots\ldots\ldots$$

$$r + \alpha_{k-2}r_1z + \alpha_{k-2}{}^2r_2z^2 + \ldots + \alpha^k{}_{k-2}r_kz^k = 0.$$

From these k equations we can always find the value of z, expressed as a rational function of the quantities $r, r_1, \ldots r_k$; and as these quantities are themselves rational functions of a, b, c, d, e, R, p, p_2, . . . , it follows that z is also a rational function of these latter quantities; but that is contrary to the hypotheses. Thus it is necessary that

$$q = 0, q_1 = 0, \ldots q_{m-1} = 0.$$

If now these equations are satisfied, it is clear that the proposed equation is satisfied by all those values which y assumes when $R^{\frac{1}{m}}$ is assigned the values

$$R^{\frac{1}{m}}, \alpha R^{\frac{1}{m}}, \alpha^2R^{\frac{1}{m}}, \ldots, \alpha^{m-1}R^{\frac{1}{m}},$$

α being a root of the equation

$$\alpha^{m-1} + \alpha^{m-2} + \ldots + \alpha + 1 = 0.$$

We also note that all the values of y are different; for otherwise we should have an equation of the same form as the equation $P = 0$, and we have just seen that such an equation leads to a contradictory result. The number m cannot exceed 5. Letting y_1, y_2, y_3, y_4, and y_5 be the roots of the proposed equation, we have

$$y_1 = p + R^{\frac{1}{m}} + p_2R^{\frac{2}{m}} + \ldots + p_{m-1}R^{\frac{m-1}{m}},$$

$$y_2 = p + \alpha R^{\frac{1}{m}} + \alpha^2pR^{\frac{2}{m}} + \ldots + \alpha^{m-1}p_{m-1}R^{\frac{m-1}{m}},$$

$$\ldots\ldots\ldots\ldots$$

$$y_m = p + \alpha^{m-1}R^{\frac{1}{m}} + \alpha^{m-2}p_2R^{\frac{2}{m}} + \ldots + \alpha p_{m-1}R^{\frac{m-1}{m}}.$$

Whence it is easily seen that

$$p = \frac{1}{m}(y_1 + y_2 + \ldots + y_m),$$

$$R^{\frac{1}{m}} = \frac{1}{m}(y_1 + \alpha^{m-1}y_2 + \ldots + \alpha y_m),$$

$$p_2R^{\frac{2}{m}} = \frac{1}{m}(y_1 + \alpha^{m-2}y_2 + \ldots + \alpha^2y_m),$$

$$\ldots\ldots\ldots\ldots$$

$$p_{m-1}R^{\frac{1}{m}} = \frac{1}{m}(y_1 + \alpha y_2 + \ldots + \alpha^{m-1}y_m).$$

Thus p, p_2, . . . p_{m-1}, R, and $R^{\frac{1}{m}}$ are rational functions of the roots of the proposed equation.

Let us now consider any one of these quantities, say R. Let

$$R = S + v^{\frac{1}{n}} + S_2v^{\frac{2}{n}} + \ldots + S_{n-1}v^{\frac{n-1}{n}}.$$

Treating this quantity as we have just treated y, we obtain the similar result that the quantities S, S_2, . . . , S_{n-1}, v, and $v^{\frac{1}{n}}$ are rational functions of the different values of R; and since these are rational functions of y_1, y_2, etc., the functions $v^{\frac{1}{n}}$, v, S, S_2 etc. have the same property. Reasoning in this way, we conclude that all the irrational functions contained in the expression for y, are rational functions of the roots of the proposed equation.

This being established, it is not difficult to complete the demonstration. Let us first consider irrational functions of the form $R^{\frac{1}{m}}$, R being a rational func-

*Source: This translation of *Mémoire sur les équations algebriques où l'on démontre l'impossibilité de la resolution de l'équation générale du cinquième degré* by W. H. Langdon with notes by Oystein Ore is taken from David Eugene Smith (ed.), *A Source Book in Mathematics* (1929), 261-266. It is reprinted by permission of McGraw-Hill Book Company, Inc. Footnotes renumbered.

tion of a, b, c, d, and e. Let $R^{\frac{1}{m}} = r$. Then r is a rational function of y_1, y_2, y_3, y_4, and y_5, and R is a symmetric function of these quantities. Now as we are interested in the solution of the general equation of the fifth degree, it is clear that we can consider y_1, y_2, y_3, y_4, and y_5 as independent variables; thus the equation $R^{\frac{1}{m}} = r$ must be satisfied under this supposition. Consequently we can interchange the quantities y_1, y_2, y_3, y_4, and y_5 in the equation $R^{\frac{1}{m}} = r$; and, remarking that R is a symmetric function, $R^{\frac{1}{m}}$ takes on m different values by this interchange. Thus the function r must have the property of assuming m values, when the five variables which it contains are permuted in all possible ways. Thus either $m = 5$, or $m = 2$, since m is a prime number, (see the memoir by M. Cauchy in the *Journal de l'école polytechnique,* vol. 17).[1] Suppose that $m = 5$. Then the function r has five different values, and hence can be put in the form

$$R^{1/5} = r = p + p_1y_1 + p_2y_1^2 + p_3y_1^3 + p_4y_1^4,$$

p, p_1, p_2, . . . being symmetric functions of y_1, y_2, etc. This equation gives, on interchanging y_1 and y_2,

$$p + p_1y_1 + p_2y_1^2 + p_3y_1^3 + p_4y_1^4 = \alpha p + \alpha p_1y_2 + \alpha p_2y_2^2 + \alpha p_3y_2^3 + \alpha p_4y_2^4,$$

where

$$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0.$$

But this equation (is impossible);[2] hence m must equal two. Then

$$R^{1/2} = r,$$

and so r must have two different values, of opposite sign. We then have,[3] (see the memoir of M. Cauchy),

$$R^{1/2} = r = v(y_1 - y_2)(y_1 - y_3) \ldots (y_2 - y_3) \ldots (y_4 - y_5) = vS^{1/2}.$$

v being a symmetric function.

Let us now consider irrational functions of the form

$$(p + p_1R^{\frac{1}{\nu}} + p_2R_1^{\frac{1}{\mu}} + \ldots)^{\frac{1}{m}},$$

p, p_1, p_2, etc., R, E_1, etc., being rational functions of a, b, c, d, and e, and consequently symmetric functions of y_1, y_2, y_3, y_4, and y_5. We have seen that it is necessary that $\nu = \mu = \ldots = 2$, $R = v^2S$, $R_1 = v_1^2S$, etc. The preceding function can thus be written in the form

$$(p + p_1S^{\frac{1}{2}})^{\frac{1}{m}},$$

Let

$$r = (p + p_1S^{\frac{1}{2}})^{\frac{1}{m}}$$

$$r_1 = (p^2 - p_1S^{\frac{1}{2}})^{\frac{1}{m}}.$$

Multiplying, we have

$$rr_1 = (p^2 - p_1^2S)^{\frac{1}{m}}.$$

If now rr_1 is not a symmetric function, m must equal two; but then r would have four different values, which is impossible; hence rr_1 must be a symmetric function. Let v be this function, then

$$r + r_1 = (p + p_1S^{\frac{1}{2}})^{\frac{1}{m}} + v(p + p_1S^{\frac{1}{2}})^{-\frac{1}{m}} = z.$$

This function having m different values, m must equal five, since m is a prime number. We thus have

$$z = q + q_1y + q_2y^2 + q_3y^3 + q_4y^4 = (p + p_1S^{1/2})^{1/5} + v(p + p_1S^{1/2})^{-1/5},$$

q, q_1, q_2, etc. being symmetric functions of y_1, y_2, y_3, etc., and consequently rational functions of a, b, c, d, and e. Combining this equation with the proposed equation, we can find y expressed as a rational function of z, a, b, c, d, and e. Now such a function can always be reduced to the form

$$y = P + R^{1/5} + P_2R^{2/5} + P_3R^{3/5} + P_4R^{4/5},$$

where P, R, P_2, P_3, and P_4 are functions of the form $p + p_1S^{1/2}$, where p, p_1, and S are rational functions of a, b, c, d, and e. From this value of y we obtain

$$R^{1/5} = \tfrac{1}{5}(y_1 + \alpha^4y_2 + \alpha^3y_3 + \alpha^2y_4 + \alpha y_5) = (p + p_1S^{1/2})^{1/5},$$

where

$$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0.$$

Now the first member has 120 different values, while the second member has only 10; hence y can not have the form that we have found: but we have proved that y must necessarily have this form, if the proposed equation can be solved: hence we conclude that

It is impossible to solve the general equation of the fifth degree in terms of radicals.

It follows immediately from this theorem, that it is also impossible to solve the general equations of degrees higher than the fifth, in terms of radicals.

NOTES

1. ["Mémoire sur le nombre des valeurs qu'une fonction peut acquérir," etc.

Let p be the greatest prime dividing n. Cauchy then proves (p. 9) that a function of n variables, taking less than p values, either is symmetric or takes only two values. In the latter case the function can be written in the form $A + B\Delta$ where A and B are symmetric, and Δ is the special two-valued function

$$\Delta = (y_1 - y_2)(y_1 - y_3) \ldots (y_{n-1} - y_n).]$$

2. [In a later paper (*Journal für die reine und angewandte Mathematik* Vol. 1, 1826) Abel gives a more detailed proof of the main theorem, based on the same principles. At the corresponding point he gives the following more elaborate proof. By considering y_1 as a common root of the given equation, the relation defining R, y_1 can be expressed in the form

$$y_1 = s_0 + s_1R^{1/5} + s_2R^{2/5} + s_3R^{3/5} + s_4R^{4/5}.$$

Substituting $\alpha^tR^{1/5}$ for R we obtain the other roots of the equation, and solving the corresponding system of five linear equations gives

$$s_1R^{1/5} = \tfrac{1}{5}(y_1 + \alpha^4y_2 + \alpha^3y_3 + \alpha^2y_4 + \alpha y_5).$$

This identity is impossible, however, since the right-hand side has 120 values, and the left-hand side has only 5.]

3. [Compare 2.]