MEMOIRE ON ALGEBRAIC EQUATIONS, IN WHICH THE IMPOSSIBILITY OF SOLVING THE GENERAL EQUATION OF DEGREE FIVE IS DEMONSTRATED .

The geometers have occupied themselves intensely with the solution of general algebraic equations, and many of them have sought to prove its impossibility; but if I am not mistaken, none of them have been successful so far. I permit myself to hope that the geometers will kindly receive this memoire, whose aim 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 degree 5, and let us suppose that it can be resolved agebraically, that is, we may express y as a function of the quantities a, b, c, d, and e, which is formed using radicals. If this is the case, it is clear that y may be brought into the form

$$y = p + p_1 R^{\frac{1}{m}} + p_2 R^{\frac{2}{m}} + \cdots + p_{m-1} R^{\frac{m-1}{m}},$$

with m being a prime number and R, p, p_1, p_2, etc. being functions of the same form as y, and so on until we reach rational functions of the quantities a, b, c, d, and e. We may suppose that it is impossible to express $R^{\frac{1}{m}}$ as a rational function of the quantities a, b, p, p_1, p_2 etc., and putting $\frac{R}{p_1^m}$ in place of R it is clear that we may assume $p_1 = 1$. We then have

$$y = p + R^{\frac{1}{m}} + p_2 R^{\frac{2}{m}} + \cdots + p_{m-1} R^{\frac{m-1}{m}}.$$

Substituting this value for y in the proposed equation, we obtain, after simplifying, an equation of the form

$$P = q + q_1 R^{\frac{1}{m}} + q_2 R^{\frac{2}{m}} + \cdots + q_{m-1} R^{\frac{m-1}{m}},$$

with q, q_1, q_2, etc. being polynomial functions of the quantities a, b, c, d, e, p, p_2, etc., and R. In order for this equation to hold it is necessary that $q = 0$, $q_1 = 0$, $q_2 = 0$ etc. $q_m = 0$. Indeed, writing z for $R^{\frac{1}{m}}$, we would have both of the equations

$$z^m - R = 0 \text{ and } q + q_1 z + \cdots + q_m z^{m-1} = 0.$$

Now, if the quantities q, q_1 etc. are not equal to zero, the equations will necessarily have one or more roots in common. Letting k be the number of these common roots, we know that it is possible to find an equation of degree k whose roots are the k aforementiond roots, and in which all of the coefficients are rational functions of R, q, q_1, et q_{m-1}. Let

$$r + r_1 z + r_2 z^2 + \cdots + r_k z^k = 0$$

be this equation. It has these roots in common with the equation $z^m - R = 0$; so all of its roots are of the form $\alpha_\mu z$, where α_μ denotes one of the roots of the equation $\alpha_\mu^m - 1 = 0$. These being substituted, we have the following equations:

$$r + r_1 z + r_2 z^2 + \cdots + r_k z^k = 0,$$

$$r + \alpha r_1 z + \alpha^2 r_2 z^2 + \cdots + \alpha^k r_k z^k = 0,$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$r + \alpha_{k-2} r_1 z + \alpha_{k-2}^2 r_2 z^2 + \cdots + \alpha_{k-2}^k r_k z^k = 0,$$

From these k equations, we can always express z as a rational function of the quantities r, r_1, r_2, etc. r_k, and since these quantities are themselves rational functions of a, b, c, d, e, $R, \ldots$ p, p_2 etc., it follows that z is also a rational function of these quantities; but this is contrary to the hypothesis. Therefore,

$$q = 0, \; q_1 = 0 \; \text{ etc. } q_{m-1} = 0.$$

Now for these equations to hold, it is clear that the proposed equation is satisfied by all the values that are obtained for y by giving $R^{\frac{1}{m}}$ the values

$$R^{\frac{1}{m}}, \alpha R^{\frac{1}{m}}, \alpha^2 R^{\frac{1}{m}}, \alpha^3 R^{\frac{1}{m}}, \text{ etc. } \alpha^{m-1} R^{\frac{1}{m}},$$

where α is a root of the equation

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

One can also see that all these values of y are different; if not then there would be an equation of the same form as the equation $P = 0$, and we have seen that any such equation leads to an impossible result. Therefore the number m cannot be greater than 5.

Denoting by y_1, y_2, y_3, y_4, y_5 the roots of the proposed equation, we have

$$y_1 = p + R^{\frac{1}{m}} + p_2 R^{\frac{2}{m}} + \cdots + p_{m-1} R^{\frac{m-1}{m}}$$

$$y_2 = p + \alpha R^{\frac{1}{m}} + p_2 \alpha^2 R^{\frac{2}{m}} + \cdots + \alpha^{m-1} p_{m-1} R^{\frac{m-1}{m}}$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$y_m = p + \alpha^{m-1} R^{\frac{1}{m}} + p_2 \alpha^{m-2} R^{\frac{2}{m}} + \cdots + \alpha p_{m-1} R^{\frac{m-1}{m}}.$$

From these equations we easily obtain

$$\begin{aligned}
p &= \frac{1}{m}\left(y_1 + y_2 + \cdots + y_m\right) \\
R^{\frac{1}{m}} &= \frac{1}{m}\left(y_1 + \alpha^{m-1} y_2 + \cdots + \alpha y_m\right) \\
p_2 R^{\frac{2}{m}} &= \frac{1}{m}\left(y_1 + \alpha^{m-2} y_2 + \cdots + \alpha^2 y_m\right) \\
&\cdots\cdots\cdots\cdots\cdots \\
p_{m-1} R^{\frac{m-1}{m}} &= \frac{1}{m}\left(y_1 + \alpha y_2 + \cdots + \alpha^{m-1} y_m\right).
\end{aligned}$$

We see from this that p, p_2 etc. 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, for example R. Let

$$R = S + v^{\frac{1}{n}} + S_2 v^{\frac{2}{n}} + \cdots + S_{n-1} v^{\frac{n-1}{n}}.$$

Treating this quantity in the same manner as y, we obtain a similar result, that $v^{\frac{1}{n}}$, v, S, S_2 etc. are rational functions of the different values of the function R; and since these are rational functions of y_1,y_2, etc., the functions $v^{\frac{1}{n}}$, v, S, S_2 etc. are as well. Following this line of reasoning, we conclude that all irrational functions contained in the expression for y are rational functions of the roots of the proposed equation.

Given this, it is not difficult to complete the proof. First consider the irrational functions of the form $R^{\frac{1}{m}}$, where R is a rational function of a, b, c, d, e. Setting $R^{\frac{1}{m}} = r$, 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, since we are trying to resolve a general equation of degree 5, it is clear that we may consider y_1, y_2, y_3, y_4, and y_5 as independent variables; the equation $R^{\frac{1}{m}} = r$ must take place within this supposition. Consequently, we may interchange the quantities y_1, y_2, y_3, y_4, and y_5 in the equation $R^{\frac{1}{m}} = r$; through these changes $R^{\frac{1}{m}}$ must take on m different values, since R is a symmetric function. The function r therefore has that property that it obtains 5 different values when we permute in all possible ways the 5 variables it contains. For this it is necessary that $m = 5$ or $m = 2$, since m is a prime number. (See the memoire of *Cauchy* in the Journal de l'école polytechnique, volume XVII).

First let us suppose that $m = 5$. Then the function r has 5 different values, and can therefore be put in the form

$$R^{\frac{1}{5}} = r = p + p_1 y_1 + p_2 y_1^2 + p_3 y_1^3 + p_4 y_1^4,$$

where $p, p_1, p_2, \ldots$ are symmetric functions of y_1, y_2, etc. Exchanging y_1 and y_2, this gives

$$p + p_1 y_1 + p_2 y_1^2 + p_3 y_1^3 + p_4 y_1^4 = \alpha p + \alpha p_1 y_2 + \alpha p_2 y_2^2 + \alpha p_3 y_2^3 + \alpha p_4 y_2^4,$$

where

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

but this equation cannot hold. The number m must therefore be equal to two. Letting

$$R^{\frac{1}{2}} = r,$$

r must have two different values of opposite sign; therefore (see the memoire of *Cauchy*)

$$R^{\frac{1}{2}} = r = v(y_1 - y_2)(y_1 - y_3)\cdots(y_2 - y_3)\cdots(y_4 - y_5) = vS^{\frac{1}{2}},$$

where v is a symmetric function.

Now let us consider the irrational functions of the form

$$\left(p + p_1 R^{\frac{1}{\nu}} + p_2 R_1^{\frac{1}{\mu}} + \cdots\right)^{\frac{1}{m}},$$

where p, p_1, p_2, etc., R, R_1 etc. are rational functions of a, b, c, d, and e, and consequently are symmetric functions of y_1, y_2, y_3, y_4, and y_5. As we have shown, we must have $\nu = \mu =$ etc. $= 2$, $R = v^2 S$, $R_1 = v_1^2 S$ etc. The function above can therefore be put in the form

$$(p + p_1 S^{\frac{1}{2}})^{\frac{1}{m}}.$$

Let

$$r = (p + p_1 S^{\frac{1}{2}})^{\frac{1}{m}},$$

$$r_1 = (p - p_1 S^{\frac{1}{2}})^{\frac{1}{m}}.$$

Multiplying, we have

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

Now if rr_1 is not a symmetric function, the number m must be equal to two, but in this case r will have four different values, which is impossible; it follows that rr_1 is a symmetric function. Letting v denote this function, consider

$$r + r_1 = (p + p_1 S^{\frac{1}{2}})^{\frac{1}{m}} + v(p + p_1 S^{\frac{1}{2}})^{\frac{-1}{m}} = z.$$

This function has m different values, and therefore $m = 5$, since m is a prime number. Consequently,

$$z = q + q_1 y + q_2 y^2 + q_3 y^3 + q_4 y^4 = (p + p_1 S^{\frac{1}{2}})^{\frac{1}{m}} + v(p + p_1 S^{\frac{1}{2}})^{\frac{-1}{m}},$$

where q, q_1, q_2, are symmetric functions of y_1,y_2,y_3, etc. and consequently rational functions of a, b, c, d, and e. Combining this with the proposed equation, we may express y as a rational function of z, a, b, c, d, and e. Such a function can always be reduced to the form

$$y = P + R^{\frac{1}{5}} + P_2 R^{\frac{2}{5}} + P_3 R^{\frac{3}{5}} + P_4 R^{\frac{4}{5}},$$

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

$$R^{\frac{1}{5}} = \frac{1}{5}(y_1 + \alpha^4 y_2 + \alpha^3 y_3 + \alpha^2 y_4 + \alpha y_5) = (p + p_1 S^{\frac{1}{2}})^{\frac{1}{5}},$$

where

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

Now the first of these functions has 120 different values and the second only has 10; consequently y cannot have the form we just found; but we have shown that y necessarily has this form, if the proposed equation is solvable. We conclude that

It is impossible to solve the general equation of degree 5 *by radicals.*

It follows immediately from this theorem that it is equally impossible to solve the general equations of degrees greater than 5 by radicals.