III.

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

Geometers have been much occupied with the general resolution of algebraic equations, and several of them have sought to prove its impossibility; but if I am not mistaken, success has not been achieved so far. I dare to hope, therefore, that geometers will receive with benevolence this paper, which aims 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 five, and let's assume that it is algebraically solvable, which means that we can express y as a function of the quantities a, b, c, d, and e formed by radicals. It is clear that in this case we can write y in the form:

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

where m is a prime number and R, p, p_1, p_2, etc. are functions of the same form as y, and so on until we get rational functions of the quantities a, b, c, d, and e. We can also assume that it is impossible to express $R^{\frac{1}{m}}$ as a rational function of the quantities a, b, etc., p, p_1, p_2, etc., and by replacing $\frac{R}{p_1^m}$ with R, it is clear that we can make $p_1 = 1$. Therefore, we have,

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

By substituting this value of y into the proposed equation, we obtain, by reducing, a result of the form,

$$P = q + q_1 R^{\frac{1}{m}} + q_2 R^{\frac{2}{m}} + \ldots + q_{m-1} R^{\frac{m-1}{m}} = 0,$$

where q, q_1, q_2, etc. are rational and integral functions of the quantities a, b, c, d, e, p, p_2, etc. and R. For this equation to hold, it is necessary that $q = 0$, $q_1 = 0$, $q_2 = 0$, etc., $q_{m-1} = 0$. Indeed, if we denote $R^{\frac{1}{m}}$ by z, we have the two equations

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

If now the quantities q, q_1, etc. are not equal to zero, these equations necessarily have one or more common roots. Letting k be the number of these roots, it is known that we can find an equation of degree k which has as its roots the k mentioned roots, and in which all of the coefficients are rational functions of R, q, q_1, and q_{m-1}. Let

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

be this equation. It has these common roots with the equation $z^m - R = 0$; yet all of the roots of that equation are of the form $\alpha_\mu z$, where α_μ denotes one of the roots of the equation $\alpha_\mu^m - 1 = 0$. Substituting, we have the following equations,

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

From these k equations, we can always obtain the value of z, expressed as a rational function of the quantities r, r_1, r_2, etc., r_k. And since these quantities themselves are rational functions of a, b, c, d, e, R, ..., p, p_2, etc., it follows that z is also a rational function of the latter quantities; but this contradicts the hypothesis. It therefore follows that

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

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

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

α being a root of the equation

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

We also see that all these values for y are different; for if not, we would have an equation of the same form as the equation $P = 0$, and such an equation leads, as we have just seen, to a result that cannot occur. Thus the number m cannot exceed 5. Therefore, denoting by y_1, y_2, y_3, y_4, and y_5 the roots of the proposed equation, we will have

$$y_1 = p + R^{\frac{1}{m}} + p_2 R^{\frac{2}{m}} + \ldots + p_{m-1} R^{\frac{m-1}{m}},$$
$$y_2 = p + \alpha R^{\frac{1}{m}} + \alpha^2 p_2 R^{\frac{2}{m}} + \ldots + \alpha^{m-1} p_{m-1} R^{\frac{m-1}{m}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$y_m = p + \alpha^{m-1} R^{\frac{1}{m}} + \alpha^{m-2} p_2 R^{\frac{2}{m}} + \ldots + \alpha p_{m-1} R^{\frac{m-1}{m}}.$$

From these equations one easily derives

$$p = \frac{1}{m} \left(y_1 + y_2 + \ldots + y_m \right),$$
$$R^{\frac{1}{m}} = \frac{1}{m} \left(y_1 + \alpha^{m-1} y_2 + \ldots + \alpha y_m \right),$$
$$p_2 R^{\frac{2}{m}} = \frac{1}{m} \left(y_1 + \alpha^{m-2} y_2 + \ldots + \alpha^2 y_m \right),$$
$$\ldots\ldots\ldots$$
$$p_{m-1} R^{\frac{m-1}{m}} = \frac{1}{m} \left(y_1 + \alpha y_2 + \ldots + \alpha^{m-1} y_m \right).$$

By this it is seen 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 way as y, we obtain the same result, namely that the quantities $v^{\frac{1}{n}}$, 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 also rational functions. Continuing this line of reasoning, 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 said, it is not difficult to complete the proof. First, let us consider the irrational functions of the form $R^{\frac{1}{m}}$, where R is a rational function of a, b, c, d, and e. Let $R^{\frac{1}{m}} = r$, where 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 dealing with the general equation of 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 hold under this assumption. Therefore, we can interchange the quantities y_1, y_2, y_3, y_4, and y_5 in the equation $R^{\frac{1}{m}} = r$. Moreover, by this

interchange, $R^{\frac{1}{m}}$ necessarily takes on m different values, it being noted that R is a symmetric function. Thus, the function r must have the property that it takes on m different values when the five variables it contains are permuted in all possible ways. For this to happen, we must have $m = 5$ or $m = 2$, it being noted that m is a prime number (cf. a memoir by Mr. *Cauchy* inserted in the Journal de l'école polytechnique, XVIIe Cahier). First let $m = 5$. Then the function r has five different values and can thus be written 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. This equation, when y_1 is replaced by y_2, 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

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

However, this equation cannot hold; consequently, the number m must be equal to two. So, let

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

where r must have two different values, which are of opposite sign. Then we have (cf. the memoire by Mr. *Cauchy*)

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

where v is a symmetric function.

Let us now consider irrational functions of the form

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

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

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

Letting

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

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

we will have by multiplying,

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

If now 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; therefore rr_1 must be a symmetric function. Letting v be this function, we will have

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

This function has m different values, so necessarily $m = 5$, it being noted that m is a prime number. We will therefore have

$$z = q + q_1 y + q_2 y^2 + q_3 y^3 + q_4 y^4 = \left(p + p_1 S^{\frac{1}{2}}\right)^{\frac{1}{5}} + v\left(p + p_1 S^{\frac{1}{2}}\right)^{-\frac{1}{5}},$$

q, q_1, q_2, etc. being symmetric functions of y_1, y_2, y_3, etc. and therefore rational functions of a, b, c, d, and e. Combining this equation with the proposed equation, we will obtain the value of y expressed as a rational function of z, a, b, c, d, and e. Now such a function is always reducible 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 $p + p_1 S^{\frac{1}{2}}$, p, p_1, and S being rational functions of a, b, c, d, and e. From this value of y we obtain

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

where

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

Now the first member has 120 different values and the second member only 10; therefore y cannot have the form we have just found; but we have demonstrated that y must necessarily have this form, if the proposed equation is solvable; therefore we conclude

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

  It follows immediately from this theorem that it is similarly impossible to solve the general equations of degrees higher than the fifth by radicals.