VII.

DEMONSTRATION OF THE IMPOSSIBILITY OF AN ALGEBRAIC RESOLUTION OF GENERAL EQUATIONS OF DEGREE GREATER THAN FOUR.

Journal for pure and applied mathematics, edited by Crelle, vol. 1, Berlin 1826.

It is known that one can solve general equations up to the fourth degree, but equations of a higher degree have only been solved in special cases. If I am not mistaken, there has not yet been a satisfactory answer to the question: "Is it possible to solve equations that go beyond the fourth degree, in general?" The purpose of this memoir is to answer that question.

Solving an equation algebraically means nothing other than expressing its roots by algebraic functions of the coefficients. It is therefore necessary to first consider the general form of algebraic functions, and then investigate whether it is possible to satisfy the given equation, by substituting the expression of an algebraic function in place of the unknown.

§I.

On the general form of algebraic functions.

Let x', x'', x''', ... be a finite number of arbitrary quantities. We say that v is an *algebraic* function of these quantities if it is possible to express v in terms of x', x'', x''', ... using the following operations: 1) addition; 2) multiplication, either with quantities dependent on x', x'', x''', ..., or with quantities that do not depend on them; 3) division; 4) extraction of roots of prime order. We did not include subtraction, raising to integer powers, and extracting roots of composite degrees among these operations as they are obviously included in the four mentioned operations.

When the function v can be formed using the first three of the above operations, it is called *algebraic and rational*, or simply *rational*; and if only the first two operations are necessary, it is called *algebraic, rational and integral*, or simply *integral*.

Let $f(x', x'', x''', \dots)$ be an arbitrary function that can be expressed as the sum of a finite number of terms of the form

$$Ax'^{m_1}x''^{m_2}\dots\dots$$

where A is a quantity independent of x', x'', etc., and where m_1, m_2, etc. are positive integers. It is clear that the first two operations described above are special cases of the operation denoted by $f(x', x'', x''', \dots)$. Therefore, integral functions, according to their definition, can be understood as resulting from a limited number of repetitions of this operation. Letting v', v'', v''', etc. denote several functions of the quantities x', x'', x''', etc., of the same form as $f(x', x'', \dots)$, the function $f(v', v'', \dots)$ will obviously be of the same form as $f(x', x'', \dots)$. Yet $f(v', v'', \dots)$ is the general expression of functions that result from the operation $f(x', x'', \dots)$ repeated twice. Therefore, the same result will always be obtained by repeating this operation as many times as desired. It follows from this that any integral function of several quantities x', x'', $\dots$ can be expressed as the sum of several terms of the form $Ax'^{m_1}x''^{m_2}\dots$.

Let us now consider rational functions. When $f(x', x'', \dots)$ and $\varphi(x', x'', \dots)$ are two integral functions, it is evident that the first three operations are particular cases of the operation denoted by

$$\frac{f(x', x'', \dots)}{\varphi(x', x'', \dots)}.$$

Therefore, we can consider a rational function as the result of the repetition of this operation. If we denote by v', v'', v''', $\dots$ several functions of the form $\frac{f(x', x'', \dots)}{\varphi(x', x'', \dots)}$, it is easy to see that the function $\frac{f(v', v'', \dots)}{\varphi(v', v'', \dots)}$ can be reduced to the same form. It follows from this that any rational function of several quantities x', x'', $\dots$ can always be reduced to the form

$$\frac{f(x', x'', \dots)}{\varphi(x', x'', \dots)},$$

where the numerator and the denominator are integral functions.

Finally, we will seek the general form of algebraic functions. Let $f(x', x'', \dots)$ be any rational function. It is clear that any algebraic function can be composed using the operation denoted by $f(x', x'', \dots)$ combined with the operation $\sqrt[m]{r}$, where m is a prime number. Therefore, if p', $p''\dots$ are rational functions of x', $x''\dots$, then

$$p_1 = f\left(x', x'', \dots, \sqrt[n']{p'}, \sqrt[n'']{p''}, \dots\right)$$

will be the general form of algebraic functions of $x', x'', \dots$, in which the operation expressed by $\sqrt[m]{r}$ only affects rational functions. Functions of the form p_1 will be called algebraic functions of the first order. By letting p_1', $p_1''\ldots$ be several quantities of the form p_1, the expression

$$p_2 = f\left(x', x'', \ldots, \sqrt[n']{p'}, \sqrt[n'']{p''}, \ldots, \sqrt[n_1']{p_1'}, \sqrt[n_1']{p_1''}, \ldots\right)$$

will be the general form of algebraic functions of $x', x'', \ldots$, in which the operation $\sqrt[m]{r}$ only affects rational functions and algebraic functions of the first order. Functions of the form p_2 will be called algebraic functions of the second order. Similarly, the expression

$$p_3 = f\left(x', x'', \ldots, \sqrt[n']{p'}, \sqrt[n'']{p''}, \ldots, \sqrt[n_1']{p_1'}, \sqrt[n_1']{p_1''}, \ldots, \sqrt[n_2']{p_2'}, \sqrt[n_2']{p_2''}, \ldots\right)$$

in which p_2', $p_2''\ldots$ are functions of the second order, will be the general form of algebraic functions of $x', x'', \ldots$, in which the operation $\sqrt[m]{r}$ only affects rational functions and algebraic functions of the first and second order.

By continuing in this way, we will obtain algebraic functions of the third, fourth…of the μ^{th} order, and it is clear that the expression for functions of the μ^{th} order will be the *general* expression of algebraic functions.

Thus, denoting by μ the order of an arbitrary algebraic function and denoting by v the function itself, we will have

$$v = f\left(r', r'' \ldots \sqrt[n']{p'}, \sqrt[n'']{p''} \ldots\right),$$

where p', $p''\ldots$ are functions of order $\mu-1$; r', $r''\ldots$ are functions of order $\mu-1$ or lower orders, and n', $n''\ldots$ are prime numbers; f still denotes a rational function of the quantities enclosed between the parentheses.

We can obviously assume that it is impossible to express one of the quantities $\sqrt[n']{p'}$, $\sqrt[n'']{p''}\ldots$ as a rational function of the others and the quantities $r', r''\ldots$; because otherwise, the function v would have the simpler form

$$v = f\left(r', r'' \ldots \sqrt[n']{p'}, \sqrt[n'']{p''} \ldots\right),$$

where the number of quantities $\sqrt[n']{p'}$, $\sqrt[n'']{p''}\ldots$ would be reduced by at least one unit. By reducing the expression of v in this way as much as possible, we would arrive at an irreducible expression, or at an expression of the form

$$v = f\left(r', r'', r''' \ldots\right);$$

but this function would only be of order $\mu-1$, while v must be of the μ^{th} order, which is a contradiction.

If in the expression of v the number of quantities $\sqrt[n']{p'}$, $\sqrt[n'']{p''}\ldots$ is equal to m, we will say that the function v is of the μ^{th} *order* and of the m^{th} *degree.* Thus we see that a function of order μ and of degree 0 is the same as a function of order $\mu-1$, and that a function of order 0 is the same as a rational function.

It follows from this, that we can write

$$v=f\left(r', r'', \ldots, \sqrt[n]{p}\right),$$

where p is a function of order $\mu-1$, but r', r'', etc. are functions of order μ and of degree at most $m-1$, and that we can always assume that it is impossible to express $\sqrt[n]{p}$ as a rational function of these quantities.

We have seen above that a rational function of several quantities can always be reduced to the form

$$\frac{s}{t},$$

where s and t are integral functions of the same variable quantities. From this, we conclude that v can always be expressed as

$$v=\frac{\varphi(r', r'' \ldots \sqrt[n]{p})}{\tau(r', r'' \ldots \sqrt[n]{p})},$$

where φ and τ denote integral functions of the quantities r', $r'' \ldots$ and $\sqrt[n]{p}$. Based on what we found earlier, any integral function of several quantities s, r', $r'' \ldots$ can be expressed in the form

$$t_0+t_1 s+t_2 s^2+\cdots+t_m s^m,$$

where t_0, $t_1 \ldots t_m$ are integral functions of r', r'', r''' $\ldots$without s. Therefore, we can set

$$v=\frac{t_0+t_1 p^{\frac{1}{n}}+t_2 p^{\frac{2}{n}}+\cdots+t_m p^{\frac{m}{n}}}{v_0+v_1 p^{\frac{1}{n}}+v_2 p^{\frac{2}{n}}+\cdots+v_{m'} p^{\frac{m'}{n}}}=\frac{T}{V},$$

where t_0, $t_1 \ldots t_m$ and v_0, $v_1 \ldots v_{m'}$ are integral functions of r', r'', r''' etc.

Let V_1, V_2, $\ldots$, V_{n-1} be the $n-1$ values of V obtained by successively substituting $\alpha p^{\frac{1}{n}}$, $\alpha^2 p^{\frac{1}{n}}$, $\alpha^3 p^{\frac{1}{n}}$, $\ldots$, $\alpha^{n-1} p^{\frac{1}{n}}$ for $p^{\frac{1}{n}}$, where α is a root of the equation $\alpha^n-1=0$ other than unity; by multiplying the numerator and denominator of $\frac{T}{V}$ by $V_1 V_2 V_3 \ldots V_{n-1}$, we obtain

$$v=\frac{T V_1 V_2 \ldots V_{n-1}}{V V_1 V_2 \ldots V_{n-1}}.$$

One knows that the product $V V_1 \ldots V_{n-1}$ can be expressed as an integral function of p and the quantities r', r'', etc., and the product $T V_1 \ldots V_{n-1}$ is, as can be seen, an integral function of $\sqrt[n]{p}$ and r', r'', etc. Assuming this product is equal to

$$s_0+s_1 p^{\frac{1}{n}}+s_2 p^{\frac{2}{n}}+\cdots+s_k p^{\frac{k}{n}},$$

we find

$$v=\frac{s_0+s_1 p^{\frac{1}{n}}+s_2 p^{\frac{2}{n}}+\cdots+s_k p^{\frac{k}{n}}}{m},$$

or, writing q_0, q_1, $q_2, \dots$ instead of $\frac{s_0}{m}$, $\frac{s_1}{m}$, $\frac{s_2}{m}$, etc.,

$$v = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_k p^{\frac{k}{n}},$$

where q_0, $q_1, \dots, q_k$ are rational functions of the quantities p, r', r'', etc.

Letting μ be an arbitrary integer, we can always write

$$\mu = an + \alpha,$$

where a and α are integers and $\alpha < n$. It follows from this that

$$p^{\frac{\mu}{n}} = p^{\frac{an+\alpha}{n}} = p^a p^{\frac{\alpha}{n}}.$$

By replacing $p^{\frac{\mu}{n}}$ with this expression in the expression for v, we obtain

$$v = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}},$$

where q_0, q_1, q_2 are still rational functions of p, r', $r'' \dots$, and therefore are functions of order μ and of degree at most $m-1$, and such that it is impossible to express $p^{\frac{1}{n}}$ rationally in terms of these quantities.

In the expression for v above, we can always set $q_1 = 1$. For if q_1 is not zero, then by setting $p_1 = p q_1^n$, we obtain

$$p = \frac{p_1}{q_1^n}, \quad p^{\frac{1}{n}} = \frac{p_1^{\frac{1}{n}}}{q_1},$$

thus

$$v = q_0 + p_1^{\frac{1}{n}} + \frac{q_2}{q_1^2} p_1^{\frac{2}{n}} + \cdots + \frac{q_{n-1}}{q_1^{n-1}} p_1^{\frac{n-1}{n}},$$

which has the same form as previous expression, except that $q_1 = 1$. If $q_1 = 0$, let q_μ be one of the quantities q_1, $q_2 \dots q_{n-1}$ that is non-zero, and let $q_\mu^n p^\mu = p_1$. From this, we deduce $q_\mu^\alpha p^{\frac{\alpha\mu}{n}} = p_1{}^{\frac{\alpha}{n}}$. So by taking two integers α and β that satisfy the equation $\alpha\mu - \beta n = \mu'$, where μ' is an integer, we have

$$q_\mu^\alpha p^{\frac{\beta n + \mu'}{n}} = p_1^{\frac{\alpha}{n}} \text{ and } p^{\frac{\mu'}{n}} = q_\mu^{-\alpha} p^{-\beta} p_1^{\frac{\alpha}{n}}.$$

By virtue of this, and noting that $q_\mu p^{\frac{1}{n}} = p_1^{\frac{1}{n}}$, v will have the form

$$v = q_0 + p_1^{\frac{1}{n}} + q_2 p_1^{\frac{2}{n}} + \cdots + q_{n-1} p_1^{\frac{n-1}{n}}.$$

From all of the above, we conclude: If v is an algebraic function of order μ and degree m, we can always write:

$$v = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + q_3 p^{\frac{3}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}},$$

where n is a prime number, q_0, $q_2 \dots q_{n-1}$ are algebraic functions of order μ and degree at most $m-1$, p is an algebraic function of order $\mu - 1$, and such that $p^{\frac{1}{n}}$ cannot be expressed rationally in terms of q_0, $q_1 \dots q_{n-1}$.

§II.

Properties of algebraic functions that satisfy a given equation.

Let

$$(1)\qquad c_0+c_1y+c_2y^2+\cdots+c_{r-1}y^{r-1}+y^r=0$$

be an arbitrary equation of degree r, where c_0, c_1, …are rational functions of x', x''…, with x', x''… being arbitrary independent quantities. Suppose that it is possible to satisfy this equation by replacing y with an algebraic function of x', x''…. Let

$$(2)\qquad y=q_0+p^{\frac{1}{n}}+q_2p^{\frac{2}{n}}+\cdots+q_{n-1}p^{\frac{n-1}{n}}$$

be this function. By substituting this expression for y into the proposed equation, we obtain, by virtue of the above, an expression of the form

$$(3)\qquad r_0+r_1p^{\frac{1}{n}}+r_2p^{\frac{2}{n}}+\cdots+r_{n-1}p^{\frac{n-1}{n}}=0,$$

where r_0, r_1, r_2, …, r_{n-1} are rational functions of p, q_0, q_1, …, q_{n-1}.

Now I claim that equation (3) cannot hold, unless we separately have

$$r_0=0,\ r_1=0,\ \ldots,\ r_{n-1}=0.$$

Indeed, in the contrary case, if we set $p^{\frac{1}{n}}=z$, we would have the two equations

$$z^n-p=0$$

and

$$r_0+r_1z+r_2z^2+\cdots+r_{n-1}z^{n-1}=0,$$

which would have one or more common roots. Leting k be the number of such roots, one knows that one can find an equation which has precisely these k roots, and whose coefficients are rational functions of p, r_0, r_1, …, r_{n-1}. Let

$$s_0+s_1z+s_2z^2+\cdots+s_{k-1}z^{k-1}+z^k=0$$

be this equation, and let

$$t_0+t_1z+t_2z^2+\cdots+t_{\mu-1}z^{\mu-1}+z^\mu$$

be a factor of its first member, such that t_0, t_1, etc., are rational functions of p, r_0, r_1, …, r_{n-1}, we likewise have

$$t_0+t_1z+t_2z^2+\cdots+t_{\mu-1}z^{\mu-1}+z^\mu=0,$$

and we assume, as we clearly may, that it is impossible to find an equation of the same form but of lower degree. The above equation has its μ roots in common with the equation $z^n-p=0$. But all the roots of the equation

$z^n - p = 0$ are of the form αz, where α is any root of unity. Therefore, noting that μ cannot be less than 2, because it is impossible to express z as a rational function of the quantities p, r_0, r_1, $\ldots$, r_{n-1}, it follows that two equations of the form

$$t_0 + t_1 z + t_2 z^2 + \cdots + t_{\mu-1} z^{\mu-1} + z^\mu = 0,$$

and

$$t_0 + \alpha t_1 z + \alpha^2 t_2 z^2 + \cdots + \alpha^{\mu-1} t_{\mu-1} z^{\mu-1} + \alpha^\mu z^\mu = 0$$

must hold. From these equations we obtain, by eliminating z^μ,

$$t_0 \left(1 - \alpha^\mu\right) + t_1 \left(\alpha - \alpha^\mu\right) z + \cdots + t_{\mu-1} \left(\alpha^{\mu-1} - \alpha^\mu\right) z^{\mu-1} = 0.$$

But since this equation has degree $\mu - 1$ and the equation

$$z^\mu + t_{\mu-1} z^{\mu-1} + \cdots = 0$$

is irreducible, and thus t_0 cannot be zero, we must have $\alpha^\mu - 1 = 0$, which does not hold. Therefore, we must have

$$r_0 = 0,\ r_1 = 0,\ \ldots,\ r_{n-1} = 0.$$

Now, given these equations, it is clear that the proposed equation will be satisfied by all the values of y obtained by assigning to $p^{\frac{1}{n}}$ the values $\alpha p^{\frac{1}{n}}$, $\alpha^2 p^{\frac{1}{n}}$, $\ldots$, $\alpha^{n-1} p^{\frac{1}{n}}$. It is easy to see that all these values of y will be different from each other; for otherwise we would have an equation of the same form as (3), but such an equation leads, as we have just seen, to contradictions.

Hence, letting y_1, $y_2 \ldots y_n$ denote n distinct roots of equation (1), we will have

$$\begin{aligned}
y_1 &= q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}}, \\
y_2 &= q_0 + \alpha p^{\frac{1}{n}} + \alpha^2 q_2 p^{\frac{2}{n}} + \cdots + \alpha^{n-1} q_{n-1} p^{\frac{n-1}{n}}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
y_n &= q_0 + \alpha^{n-1} p^{\frac{1}{n}} + \alpha^{n-2} q_2 p^{\frac{2}{n}} + \cdots + \alpha q_{n-1} p^{\frac{n-1}{n}}.
\end{aligned}$$

From these n equations, one can easily deduce

$$\begin{aligned}
q_0 &= \frac{1}{n}\left(y_1 + y_2 + y_3 + \cdots + y_n\right), \\
p^{\frac{1}{n}} &= \frac{1}{n}\left(y_1 + \alpha^{n-1} y_2 + \alpha^{n-2} y_3 + \cdots + \alpha y_n\right), \\
q_2 p^{\frac{2}{n}} &= \frac{1}{n}\left(y_1 + \alpha^{n-2} y_2 + \alpha^{n-4} y_3 + \cdots + \alpha^2 y_n\right), \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
q_{n-1} p^{\frac{n-1}{n}} &= \frac{1}{n}\left(y_1 + \alpha y_2 + \alpha^2 y_3 + \cdots + \alpha^{n-1} y_n\right).
\end{aligned}$$

We see by this that all quantities $p^{\frac{1}{n}}$, q_0, $q_2 \ldots q_{n-1}$ are rational functions of the roots of the proposed equation. Indeed, we have

$$q_\mu = n^{\mu-1}\frac{y_1+\alpha^{-\mu}y_2+\alpha^{-2\mu}y_3+\cdots+\alpha^{-(n-1)\mu}y_n}{(y_1+\alpha^{-1}y_2+\alpha^{-2}y_8+\cdots+\alpha^{-(n-1)}y_n)^\mu}.$$

Let us now consider the general equation of degree m,

$$0 = a + a_1x + a_2x^2 + \cdots + a_{m-1}x^{m-1} + x^m,$$

and suppose it is algebraically solvable. Let

$$x = s_0 + v^{\frac{1}{n}} + s_2v^{\frac{2}{n}} + \cdots + s_{n-1}v^{\frac{n-1}{n}};$$

by what is above, the quantities v, s_0, s_2, etc. can be expressed rationally in terms of x_1, $x_2 \ldots x_m$, where x_1, $x_2 \ldots x_m$ denote the roots of the proposed equation.

Let us now consider any of the quantities v, s_0, s_2, etc., for example v. If we denote by $v_1, v_2, \ldots, v_{n'}$ the distinct values of v obtained by exchanging the roots $x_1, x_2, \ldots, x_m$ in all possible ways, we can form an equation of degree n' whose coefficients are rational functions of $a, a_1, \ldots, a_{n-1}$, and whose roots are the quantities $v_1, v_2, \ldots, v_{n'}$, which are rational functions of the quantities $x_1, x_2, \ldots, x_m$.

Therefore, if

$$v = t_0 + u^{\frac{1}{\nu}} + t_2u^{\frac{2}{\nu}} + \cdots + t_{\nu-1}u^{\frac{\nu-1}{\nu}},$$

then all the quantities $u^{\frac{1}{\nu}}$, t_0, $t_2 \ldots t_{\nu-1}$ will be rational functions of v_1, $v_2 \ldots v_{n'}$, and consequently of x_1, $x_2 \ldots x_m$. By treating the quantities u, t_0, t_2, etc. in the same way, we can conclude that

> if an equation is algebraically solvable, we can always give the root a form in which all the algebraic functions of which it is composed can be expressed as rational functions of the roots of the proposed equation.

§III.

On the number of different values that a function of several quantities can take when the quantities it contains are exchanged with each other.

Let v be a rational function of several independent quantities x_1, $x_2 \ldots x_n$. The number of different values that this function can take by exchanging the quantities on which it depends cannot exceed the product $1.2.3 \ldots n$. Let μ be this product.

Now let $v\begin{pmatrix}\alpha & \beta & \gamma & \delta & \dots \\ a & b & c & d & \dots\end{pmatrix}$ be the value that an arbitrary function v receives when x_a, x_b, x_c, x_d, etc. are substituted in place of x_α, x_β, x_γ, x_δ, etc. Denoting by A_1, $A_2 \dots A_\mu$ the various permutations of μ that can be formed with indices 1, 2, $3 \dots n$, it is clear that the different values of v can be expressed as

$$v\begin{pmatrix}A_1\\A_1\end{pmatrix}, v\begin{pmatrix}A_1\\A_2\end{pmatrix}, v\begin{pmatrix}A_1\\A_3\end{pmatrix} \dots . v\begin{pmatrix}A_1\\A_u\end{pmatrix}.$$

Supposing that the number of different values of v is less than μ, it must be that several values of v are equal to each other, so for example

$$v\begin{pmatrix}A_1\\A_1\end{pmatrix} = v\begin{pmatrix}A_1\\A_2\end{pmatrix} = \dots = v\begin{pmatrix}A_1\\A_m\end{pmatrix}.$$

If we apply to these quantities the substitution denoted by $\begin{pmatrix}A_1\\A_{m+1}\end{pmatrix}$, we will have this new series of equal values

$$v\begin{pmatrix}A_1\\A_{m+1}\end{pmatrix} = v\begin{pmatrix}A_1\\A_{m+2}\end{pmatrix} = \dots = v\begin{pmatrix}A_1\\A_{2m}\end{pmatrix},$$

which are different from the first ones, but in the same number. By changing these quantities again using the substitution denoted by $\begin{pmatrix}A_1\\A_{2m+1}\end{pmatrix}$, we will have a new system of equal quantities, but different from the previous ones. By continuing this process until all possible permutations have been exhausted, the μ values of v will be divided into several systems, each of which will contain precisely m equal values. It follows from this that if we represent the number of different values of v by ϱ, which is equal to the number of systems, we will have

$$\varrho m = 1.2.3 \dots n,$$

that is:

The number of different values that a function of n quantities can take on from all possible substitutions of these quantities, is necessarily a divisor of the product $1.2.3 \dots n$. This is well known.

Let us now consider an arbitrary substitution $\begin{pmatrix}A_1\\A_m\end{pmatrix}$. Suppose that by applying it repeatedly to the function v, we obtain the sequence of values

$$v,\ v_1,\ v_2 \dots v_{p-1},\ v_p,$$

Then it is clear that v will necessarily be repeated multiple times. When v returns after a number p of substitutions, we say that $\begin{pmatrix}A_1\\A_m\end{pmatrix}$ is a *recurrent* *substitution of order p.* Therefore, we have this periodic series

$$v,\ v_1,\ v_2 \dots v_{p-1},\ v,\ v_1,\ v_2 \dots$$

or, if we represent by $v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^r$ the value of v obtained after repeatedly applying the substitution designated by $\begin{pmatrix} A_1 \\ A_m \end{pmatrix}$ r times, we have the series

$$v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^0, v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^1, v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^2 \dots v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{p-1}, v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^0 \dots$$

It follows that

$$v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{\alpha p+r} = v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^r$$

$$v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{\alpha p} = v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^0 = v.$$

Now let p be the greatest prime number less than or equal to n. If the number of different values of v is less than p, it must be the case that among p arbitrary values, two are equal to each other.

It therefore follows that among the p values,

$$v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^0, v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^1, v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^2 \dots v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{p-1},$$

two will be equal to each other. Supposing for example that

$$v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^r = v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{r'},$$

we conclude that

$$v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{r+p-r} = v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{r'+r-r}.$$

Writing r instead of $r'+p-r$ and noticing that $v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^p = v$, we infer

$$v = v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^r,$$

where r is obviously not a multiple of p. The value of v is therefore not changed by the substitution $\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^r$, nor consequently by the repetition of the same substitution. We thus have

$$v = v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{r\alpha},$$

where α is an integer. Now if p is a prime number, it is evident that we can always find two integers α and β such that

$$r\alpha = p\beta + 1,$$

so

$$v = v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{p\beta+1},$$

and since

$$v = v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{p\beta},$$

we have

$$v = v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}.$$

The value of v is therefore not changed by the recurrent substitution $\begin{pmatrix} A_1 \\ A_m \end{pmatrix}$ of order p.

Now it is clear that

$$\begin{pmatrix} \alpha & \beta & \gamma & \delta & \dots & \zeta & \eta \\ \beta & \gamma & \delta & \epsilon & \dots & \eta & \alpha \end{pmatrix} \text{ and } \begin{pmatrix} \beta & \gamma & \delta & \epsilon & \dots & \eta & \alpha \\ \gamma & \alpha & \beta & \delta & \dots & \zeta & \eta \end{pmatrix}$$

are recurrent substitutions of order p, when p is the number of indices α, β, $\gamma \dots \eta$. The value of v will therefore not be changed either by the combination of these two substitutions. These two substitutions are obviously equivalent to

$$\begin{pmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \end{pmatrix},$$

and this one to the following two applied successively,

$$\begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} \text{ and } \begin{pmatrix} \beta & \gamma \\ \gamma & \beta \end{pmatrix}.$$

The value of v will therefore not be changed by the combination of these two substitutions. Hence

$$v = v\begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}\begin{pmatrix} \beta & \gamma \\ \gamma & \beta \end{pmatrix};$$

Similarly

$$v = v\begin{pmatrix} \beta & \gamma \\ \gamma & \beta \end{pmatrix}\begin{pmatrix} \gamma & \delta \\ \delta & \gamma \end{pmatrix},$$

from which we deduce

$$v = v\begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}\begin{pmatrix} \gamma & \delta \\ \delta & \gamma \end{pmatrix}.$$

We see from this that the function v is not changed by two successive substitutions of the form $\begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}$, where α and β are arbitrary indices. If such a substitution is called a *transposition*, we can conclude that any given value of v is not changed by an even number of transpositions, and consequently all values of v resulting from an odd number of transpositions are equal. Any interchange of the elements of a function can be accomplished using a certain number of transpositions; therefore the function v cannot have more than two different values. From this we deduce the following theorem:

> The number of different values that a function of n quantities can take cannot be reduced to less than the largest prime number that does not exceed n, unless it reduces to 2 or 1.

It is therefore impossible to find a function of 5 quantities that has 3 or 4 different values.

The proof of this theorem is taken from a paper by Mr. *Cauchy* inserted in cahier XVII of the Journal de l'école polytechnique p. 1.

Now let v and v' be two functions, each having two different values. Denoting these double values by v_1, v_2, and v_1', v_2', it follows from the above that the two expressions

$$v_1 + v_2 \quad \text{and} \quad v_1 v_1' + v_2 v_2'$$

will be symmetric functions. Letting

$$v_1 + v_2 = t \quad \text{and} \quad v_1 v_1' + v_2 v_2' = t_1,$$

we obtain

$$v_1 = \frac{t v_2' - t_1}{v_2' - v_1'}.$$

Now, let the number of quantities $x_1, x_2, \ldots, x_m$ be equal to five. The product

$$\varrho = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)(x_2 - x_3)(x_3 - x_4)(x_2 - x_5)(x_3 - x_4)(x_3 - x_5)(x_4 - x_5)$$

will obviously be a function that has two different values; the second value being the same function with the opposite sign. Therefore, by setting $v_1' = \varrho$, we will have $v_2' = -\varrho$. The expression for v_1 will thus be

$$v_1 = \frac{t_1 + \varrho t}{2\varrho},$$

or alternatively

$$v_1 = \frac{1}{2} t + \frac{t_1}{2\varrho^2} \varrho,$$

where $\frac{1}{2}t$ is a symmetric function; ϱ has two values that only differ in sign, so that $\frac{t_1}{2\varrho^2}$ is also a symmetric function. Therefore, by setting $\frac{1}{2}t = p$ and $\frac{t_1}{2\varrho^2} = q$, it follows that

> any function of five quantities that has two different values can be expressed in the form $p + q\varrho$, where p and q are both symmetric functions and $\varrho = (x_1 - x_2)(x_1 - x_3)\dots(x_4 - x_5)$.

To achieve our goal, we still need the general form of functions of five variables that have five different values. We can find it as follows:

Let v be a rational function of the quantities x_1, x_2, x_3, x_4, x_5 which has the property of being invariant when four of the five quantities are exchanged, for example x_2, x_3, x_4, x_5. Under this condition, v will obviously be symmetric with respect to x_2, x_3, x_4, x_5. Therefore, v can be expressed as a rational function of x_1 and symmetric functions of x_2, x_3, x_4, x_5. But any symmetric function of these quantities can be expressed as a rational function of the coefficients of a fourth degree equation, whose roots are x_2, x_3, x_4, x_5. Thus, by setting

$$(x - x_2)(x - x_3)(x - x_4)(x - x_5) = x^4 - px^3 + qx^2 - rx + s,$$

the function v can be expressed rationally in terms of x_1, p, q, r, s. Now, if we set

$$(x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5) = x^5 - ax^4 + bx^3 - cx^2 + dx - e,$$

we will have

$$\begin{aligned}(x - x_1)\left(x^4 - px^3 + qx^3 - rx + s\right) &= x^5 - ax^4 + bx^3 - cx^2 + dx - e\\ &= x^5 - (p + x_1)x^4 + (q + px_1)x^3 - (r + qx_1)x^2 + (s + rx_1)x - sx_1,\end{aligned}$$

from which we deduce that

$$\begin{aligned}p &= a - x_1,\\ q &= b - ax_1 + x_1^2,\\ r &= c - bx_1 + ax_1^3 - x_1^3,\\ s &= d - cx_1 + bx_1^2 - ax_1^3 + x_1^4;\end{aligned}$$

therefore, the function v can be expressed rationally in terms of x_1, a, b, c, d.

From there it follows that the function v can be written in the form

$$v = \frac{t}{\varphi x_1},$$

where t and φx_1 are two integral functions of x_1, a, b, c, d. Multiplying the numerator and the denominator of this function by φx_2, φx_3, φx_4, φx_5, we have

$$v = \frac{t.\varphi x_2.\varphi x_3.\varphi x_4.\varphi x_5}{\varphi x_1.\varphi x_2.\varphi x_3.\varphi x_4.\varphi x_5}.$$

Now one can see that $\varphi x_2 . \varphi x_3 . \varphi x_4 . \varphi x_5$ is an integral and symmetric function of x_2, x_3, x_4, x_5. Therefore, we can express this product as an integral function of p, q, r, s, and hence as an integral function of x_1, a, b, c, d. The numerator of the above fraction is therefore an integral function of the same quantities; the denominator is a symmetric function of x_1, x_2, x_3, x_4, x_5 and therefore it can be expressed as a rational function of a, b, c, d, e. We can thus write

$$v = r_0 + r_1 x_1 + r_2 x_1^2 + \cdots + r_m x_1^m .$$

By multiplying the equation

$$x_1^5 = a x_1^4 - b x_1^3 + c x_1^2 - d x_1 + e$$

successively by x_1, $x_1^2 \ldots x_1^{m-5}$, it is clear that we will obtain $m-4$ equations, from which we will obtain expressions for x_1^5, $x_1^6 \ldots x_1^m$ of the form

$$\alpha + \beta x_1 + \gamma x_1^2 + \delta x_1^3 + \varepsilon x_1^4 ,$$

where α, β, γ, δ, ε are rational functions of a, b, c, d, e.

We can thus reduce v to the form

$$\text{(a)} \qquad v = r_0 + r_1 x_1 + r_2 x_1^2 + r_3 x_1^3 + r_4 x_1^4 ,$$

where r_0, r_1, r_2, etc. are rational functions of a, b, c, d, e, that is, symmetric functions of x_1, x_2, x_3, x_4, x_5.

This is the general form of functions that are not altered when exchanging the quantities x_2, x_3, x_4, x_5 among themselves. Either they have five distinct values, or they are symmetric.

Now let v be a rational function of x_1, x_2, x_3, x_4, x_5, which has five values v_1, v_2, v_3, v_4, v_5. Consider the function $x_1^m v$. By exchanging the four quantities x_2, x_3, x_4, x_5 among themselves in all possible ways, the function $x_1^m v$ will always have one of the following values

$$x_1^m v_1 ,\ x_1^m v_2 ,\ x_1^m v_3 ,\ x_1^n v_4 ,\ x_1^m v_5 .$$

Now I say that the number of distinct values of $x_1^m v$ resulting from these changes will be less than five. Indeed, if all five values were to occur, we would obtain 20 new values from these values by successively exchanging x_1 with x_2, x_3, x_4, x_5, which would necessarily be different from each other and from the previous values. Thus, the function would have a total of 25 distinct values, which is impossible since 25 is not a divisor of the product 1.2.3.4.5. Therefore, denoting by μ the number of values that v can take when we exchange the quantities x_2, x_3, x_4, x_5 with each other in all possible ways, μ must have one of the following four values: 1, 2, 3, 4.

1. If $\mu = 1$, then according to the preceding, v will be of the form (a).

2. If $\mu = 4$, then the sum $v_1 + v_2 + v_3 + v_4$ will be a function of the form (a). Now we have $v_5 = (v_1 + v_2 + v_3 + v_4 + v_5) - (v_1 + v_2 + v_3 + v_4) =$ a symmetric function minus $(v_1 + v_2 + v_3 + v_4)$; hence v_5 is of the form (a).

3. If $\mu = 2$, then $v_1 + v_2$ will be a function of the form (a). Therefore,

$$v_1 + v_2 = r_0 + r_1 x_1 + r_2 x_1^2 + r_3 x_1^3 + r_4 x_1^4 = \varphi x_1.$$

By successively exchanging x_1 with x_2, x_3, x_4, x_5, we have

$$\begin{aligned} & v_1 + v_2 = \varphi x_1, \\ & v_2 + v_3 = \varphi x_2, \\ & \dots\dots\dots\dots \\ & v_{m-1} + v_m = \varphi x_{m-1}, \\ & v_m + v_1 = \varphi x_m, \end{aligned}$$

where m is one of the numbers 2, 3, 4, 5. For $m = 2$, we have $\varphi x_1 = \varphi x_2$, which is impossible because the number of values of φx_1 must be five. For $m = 3$ we have

$$v_1 + v_2 = \varphi x_1,\ v_2 + v_3 = \varphi x_2,\ v_3 + v_1 = \varphi x_3,$$

from which we deduce

$$2v_1 = \varphi x_1 - \varphi x_2 + \varphi x_3.$$

But the right hand side of this equation has more than 5 values, since it has 30. We can prove in the same way that m cannot be equal to 4 or 5. It follows from this that μ is not equal to 2.

4. Let $\mu = 3$. In this case, $v_1 + v_2 + v_3$ and consequently $v_4 + v_5 = (v_1 + v_2 + v_3 + v_4 + v_5) - (v_1 + v_2 + v_3)$ will have five values. But we have just seen that this assumption is inadmissible. Therefore μ cannot be equal to 3. From all of this, we deduce the following theorem:

> Any rational function in five quantities, which has five distinct values, will necessarily have the form
>
> $$r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4$$
>
> where r_0, r_1, r_2, etc. are symmetric functions, and x is any one of the five quantities.

From the equation

$$r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4 = v$$

we can easily deduce, using the proposed equation, an expression for the value of x of the form

$$x = s_0 + s_1 v + s_2 v^2 + s_3 v^3 + s_4 v^4,$$

where s_0, s_1, s_2, etc., as well as r_0, r_1, r_2, etc., are symmetric functions.

Let v be a rational function with m different values v_1, v_2, $v_3 \dots v_m$. Setting

$$\begin{aligned}&(v - v_1)(v - v_2)(v - v_3) \dots (v - v_m)\\&= q_0 + q_1 v + q_2 v^2 + \dots + q_{m-1} v^{m-1} + v^m = 0,\end{aligned}$$

we know that $q_0, q_1, q_2 \dots$ are symmetric functions, and that the m roots of the equation are $v_1, v_2, v_3 \dots v_m$. Now I claim that it is impossible to express the value of v as a root of an equation of the same form, but of lower degree. Indeed, suppose that

$$t_0 + t_1 v + t_2 v^2 + \dots + t_{\mu-1} v^{\mu-1} + v^\mu = 0$$

is such an equation, where t_0, t_1, etc. are symmetric functions, and let v_1 be a value of v that satisfies this equation. Then we have

$$v^\mu + t_{\mu-1} v^{\mu-1} + \dots = (v - v_1) P_1.$$

By interchanging the elements of the function, we obtain the following series of equations:

$$\begin{aligned}&v^\mu + t_{\mu-1} v^{\mu-1} + \dots = (v - v_2) P_2,\\&v^\mu + t_{\mu-1} v^{\mu-1} + \dots = (v - v_3) P_3,\\&\dots\dots\dots\dots\dots\dots\\&v^\mu + t_{\mu-1} v^{\mu-1} + \dots = (v - v_m) P_m,\end{aligned}$$

It follows that $v - v_1$, $v - v_2$, $v - v_3 \dots v - v_m$ will be factors of $v^\mu + t_{\mu-1} v^{\mu-1} + \dots$ and therefore μ must necessarily be equal to m. We deduce the following theorem:

> When a function of several quantities has m distinct values, one can always find an equation of degree m, whose coefficients are symmetric functions, and which has these values as roots; but it is impossible to find an equation of the same form of a lower degree that has one or more of these values as roots.

§IV.

Proof of the impossibility of the general resolution of the equation of the fifth degree.

According to the propositions found above, we can state the following theorem:

"It is impossible to solve general equations of the fifth degree."

According to §II, all the algebraic functions of which an algebraic expression for the roots is composed can be expressed as rational functions of the roots of the proposed equation.

As it is impossible to express the root of an equation generally by a rational function of the coefficients, we must have

$$R^{\frac{1}{m}} = v,$$

where m is a prime number and R is a rational function of the coefficients of the proposed equation, that is to say, a symmetric function of the roots; v is a rational function of the roots. We conclude that

$$v^m - R = 0.$$

By virtue of §II, it is impossible to lower the degree of this equation; therefore, the function v must, according to the last theorem of the preceding paragraph, have m different values. Since m must be a divisor of the product 1.2.3.4.5, this number can be equal to 2 or 3 or 5. However (§III), there is no five-variable function that has 3 values: therefore, we must have $m = 5$ or $m = 2$. Let $m = 5$, then we have as a result of the previous paragraph

$$\sqrt[5]{R} = r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4,$$

from which

$$x = s_0 + s_1 R^{\frac{1}{5}} + s_2 R^{\frac{2}{5}} + s_3 R^{\frac{3}{5}} + s_4 R^{\frac{4}{5}}.$$

We derive from this (§II)

$$s_1 R^{\frac{1}{5}} = \frac{1}{5}\left(x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^2 x_4 + \alpha x_5\right)$$

where $\alpha^5 = 1$. This equation is impossible, since the second member has 120 values and yet it must be a root of a fifth-degree equation $z^5 - s_1^5 R = 0$. Therefore, we must have $m = 2$.

Therefore we have (§II)

$$\sqrt{R} = p + qs,$$

where p and q are symmetric functions, and

$$s = (x_1 - x_2)\ldots(x_4 - x_5).$$

We obtain, by exchanging x_1 and x_2 with each other,

$$-\sqrt{R} = p - qs,$$

from which we deduce $p=0$ and $\sqrt{R}=qs$. By this, we see that any algebraic function of the first order that is found in the expression of the root must necessarily have the form $\alpha+\beta\sqrt{s^2}=a+\beta s$, where α and β are symmetric functions. However, it is impossible to express the roots by a function of the form $\alpha+\beta\sqrt{R}$; there must therefore be an equation of the form

$$\sqrt[m]{\alpha+\beta\sqrt{s^2}}=v,$$

where α and β are nonzero, m is a prime number, α and β are symmetric functions, and v is a rational function of the roots. This gives

$$\sqrt[m]{\alpha+\beta s}=v_1, \ \sqrt[m]{\alpha-\beta s}=v_2,$$

where v_1 and v_2 are rational functions. By multiplying v_1 by v_2, we have

$$v_1v_2=\sqrt[m]{\alpha^2-\beta^2s^2}$$

Now $\alpha^2-\beta^2s^2$ is a symmetric function. If now $\sqrt[m]{\alpha^2-\beta^2s^2}$ is not a symmetric function, the number m, according to the above, must be equal to two. But in this case, v will be equal to $\sqrt{\alpha+\beta\sqrt{s^2}}; v$ will therefore have four different values, which is impossible.

Therefore, $\sqrt[m]{\alpha^2-\beta^2s^2}$ must be a symmetric function. Let γ be this function, then we have

$$v_2v_1=\gamma, \quad \text{and} \quad v_2=\frac{\gamma}{v_1}.$$

Let

$$v_1+v_2=\sqrt[m]{\alpha+\beta\sqrt{s^2}}+\frac{\gamma}{\sqrt{\alpha+\beta\sqrt{s^2}}}=p=\sqrt[m]{R}+\frac{\gamma}{\sqrt[m]{R}}=R^{\frac{1}{m}}+\frac{\gamma}{R}R^{\frac{m-1}{m}}.$$

Let p_1, p_2, $p_3\ldots p_m$ denote the different values of p resulting from the successive substitution of $\alpha R^{\frac{1}{m}}$, $\alpha^2R^{\frac{1}{m}}$, $\alpha^3R^{\frac{1}{m}}\ldots\alpha^{m-1}R^{\frac{1}{m}}$ in place of $R^{\frac{1}{m}}$, where α satisfies the equation

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

and take the product

$$(p-p_1)(p-p_2)\ldots(p-p_m)=p^m-Ap^{m-1}+A_1p^{m-2}-\cdots=0.$$

It is easy to see that A, A_1, etc. are rational functions of the coefficients of the proposed equation and therefore symmetric functions of the roots. This equation is clearly irreducible. It is therefore necessary, according to the last theorem of the previous paragraph, that p, considered as a function of the roots, has m different values. We conclude that $m=5$. But in this case p will be of the form (a) of the previous paragraph. Therefore, we will have

$$\sqrt[5]{R}+\frac{\gamma}{\sqrt[5]{R}}=r_0+r_1x+r_2x^2+r_3x^3+r_4x^4=p,$$

from which

$$x = s_0 + s_1 p + s_2 p^2 + s_3 p^3 + s_4 p^4,$$

that is, by replacing p with $R^{\frac{1}{5}} + \frac{\gamma}{R} R^{\frac{4}{5}}$,

$$x = t_0 + t_1 R^{\frac{1}{5}} + t_2 R^{\frac{2}{5}} + t_3 R^{\frac{3}{5}} + t_4 R^{\frac{4}{5}}$$

where t_0, t_1, t_2, etc. are rational functions of R and the coefficients of the proposed equation. We deduce (§II)

$$t_1 R^{\frac{1}{5}} = \frac{1}{5}\left(x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^2 x_4 + \alpha x_5\right) = p',$$

where

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

From the equation $p' = t_1 R^{\frac{1}{5}}$ we obtain $p'^5 = t_1^5 R$. But since $t_1^5 R$ is of the form $u + u'\sqrt{s^2}$, we have $p'^5 = u + u'\sqrt{s^2}$, which gives

$$\left(p'^5 - u\right)^2 = u'^2 s^2.$$

This equation gives p' in terms of a tenth-degree equation, all of whose coefficients are symmetric functions. But according to the last theorem of the previous paragraph, this is impossible; for since

$$p' = \frac{1}{5}\left(x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^2 x_4 + \alpha x_5\right),$$

p' would have 120 different values, which is a contradiction.

We therefore conclude that it is impossible to algebraically solve the general equation of the fifth degree.

It immediately follows from this theorem that it is also impossible to algebraically solve the general equations of degrees greater than five. Therefore, the equations of the first four degrees are the only ones that can be algebraically solved in a general manner.

APPENDIX.

ANALYSIS OF THE PREVIOUS MEMOIR.

Bulletin of mathematical, astronomical, physical and chemical sciences published by B$^{\text{on}}$ de *Férussac*, vol. 6, p. 347; Paris 1826.

The author demonstrates in this paper that it is impossible to algebraically solve the general equation of the fifth degree; because any algebraic function of the proposed coefficients, when substituted in place of the unknown, leads to an absurdity. In a first paragraph, the author seeks the general expression of algebraic functions of several quantities, based on the definition that an algebraic function results from 1° addition, 2° multiplication, 3° division, and 4° extraction of roots whose exponents are *prime* numbers. Subtractions, raising to powers, and extracting roots with *composite* exponents fall into the previous operations. Hence it follows that 1° any *rational and integral* function of the quantities x_1, x_2, x_3, etc., that is, any function that can be formed by means of the *first two* mentioned operations, can be expressed as a sum of a *finite* number of terms of the form $Ax_1^{m_1}x_2^{m_2}\ldots$, where A is a constant and m_1, $m_2, \ldots$ are integers; 2° any *rational* function of the same quantities, that is, any function that can be formed by means of the *first three* operations, can be expressed as a quotient of two integral functions; 3° any algebraic function can be formed by repetitions of the operations indicated by

$$(1) \qquad p' = f(x_1, x_2, x_3 \ldots p_1^{\frac{1}{n_1}}, p_2^{\frac{1}{n_2}}, \ldots),$$

where f denotes a rational function of the quantities in parentheses; p_1, $p_2, \ldots$ are rational functions of x_1, $x_2 \ldots$, and $n_1, n_2, \ldots$ are prime numbers. For the sake of brevity, we will refer to such a function p' as an *algebraic function of the first order.* If now we were to form a new function in which first-order functions entered in the same way as p_1, $p_2 \ldots$ enter in p', we would have a *algebraic function of the second order*; and, in general, a function of order

μ would be one that could contain functions of all orders up to order $\mu-1$, combined *algebraically* with each other. Of course, this function of order μ cannot be reduced to a lower order by reducing the functions that compose it. Furthermore, if this same function of order μ contains m quantities of that order, we will say that it is of the m^{th} *degree:* and by denoting it by v, we can write

$$(2) \qquad v = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}}$$

that is, we have this first *theorem: Every algebraic function v of order μ and degree m can be represented by formula (2), where n is a prime number, q_1, $q_2, \ldots q_{n-1}$ are algebraic functions of order μ and degree at most $m-1$, and p is an algebraic function of order $\mu-1$, such that it is impossible to express $p^{\frac{1}{n}}$ as a rational function of p, q_0, $q_2, \ldots, q_{n-1}$.*

After thus finding the general expression of algebraic functions, the author considers, in a second paragraph, an arbitrary equation whose coefficients are rational functions of the quantities x_1, $x_2 \ldots$ and that we suppose to be algebraically solvable. Then denoting the unknown by y, and by

$$(3) \qquad \varphi(x_1, x_2, x_3 \ldots y) = 0,$$

the equation itself, it is necessary that the first member can be reduced to zero, by putting for y a certain function of the form (2). By this substitution, the equation (3) will be transformed into another of the form

$$(4) \qquad r_0 + r_1 p^{\frac{1}{n}} + r_2 p^{\frac{2}{n}} + \cdots + r_{n-1} p^{\frac{n-1}{n}} = 0,$$

where r_0, r_1, r_2, $r_3 \ldots$ are rational functions of x_1, x_2, $x_3 \ldots$ and of q_0, q_2, $q_3 \ldots$ This equation implies the following ones:

$$(5) \qquad r_0 = 0,\ r_1 = 0,\ r_2 = 0,\ \ldots r_{n-1} = 0,$$

because otherwise, the equation (4) could give the value of $p^{\frac{1}{n}}$ as a *rational* function of p, r_0, $r_1 \ldots r_{n-1}$, which contradicts the statement of the previous theorem. If the equations (5) hold, the equation (4), and hence the equation (3), will be satisfied by all values of y that we obtain by putting, instead of $p^{\frac{1}{n}}$, the $n-1$ values $\alpha p^{\frac{1}{n}}$, $\alpha^2 p^{\frac{1}{n}}, \ldots . \alpha^{n-1} p^{\frac{1}{n}}$, where α is an imaginary root of unity. By this we obtain the values of the n roots of the equation (3), namely

$$y_1 = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}},$$

$$y_2 = q_0 + \alpha p^{\frac{1}{n}} + \alpha^2 q_2 p^{\frac{2}{n}} + \cdots + \alpha^{n-1} q_{n-1} p^{\frac{n-1}{n}},$$

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

$$y_n = q_0 + \alpha^{n-1} p^1 + \alpha^{n-2} q_2 p^{\frac{1}{n}} + \ldots \cdots + \alpha q_{n-1} p^{\frac{n-1}{n}};$$

these equations give the n quantities $p^{\frac{1}{n}}$, q_0, $q_2 \dots q_{n-1}$ as *rational* functions of the roots y_1, $y_2 \dots y_n$.

If now $fx = 0$ is a general algebraic equation, solvable *algebraically*, and x_1, $x_2 \dots$ are the roots of this equation, we must have

$$x = s_0 + v^{\frac{1}{n}} + s_2 v^{\frac{2}{n}} + \cdots + s_{n-1} v^{\frac{n-1}{n}},$$

this formula being analogous to formula (2). According to what we have just seen, $v^{\frac{1}{n}}$, s_0, $s_2 \dots s_{n-1}$ will be rational functions of the roots of the proposed equation. With this in mind, let us consider any of the quantities v, s_0, $s_2 \dots s_{n-1}$, for example v; denoting by n' the number of all *distinct* values of v, that can be obtained by exchanging in every possible way the roots of the proposed equation, we can form an equation of degree n' that has all these values as roots, and whose coefficients are rational and symmetric functions of the values of v, and therefore are rational functions of x_1, $x_2 \dots$ Then setting

$$v = t_0 + u^{\frac{1}{\nu}} + t_2 u^{\frac{2}{\nu}} + \cdots + t_{v-1} u^{\frac{\nu-1}{\nu}},$$

all of the quantities u, t_0, $t_2 \dots t_{\nu-1}$ will be rational functions of the values of v, and therefore of $x_1, x_2 \dots$ By continuing this reasoning, we establish the following theorem:

Second theorem: If an algebraic equation is algebraically solvable, it is always possible to give the root a form such that all the algebraic expressions of which it is composed can be expressed by rational functions of the roots of the proposed equation.

In the third paragraph it is proved, following a paper by Mr. *Cauchy* inserted in cahier XVII of the *Journal de l'École Polytechnique*, that: 1° the number of values of a rational function of n quantities cannot be reduced below the largest prime number less than or equal to n without becoming equal to 2 or 1; 2° any rational function that has two different values will have the form

$$p + q\,(x_1 - x_2)\,(x_1 - x_3) \dots (x_2 - x_3) \dots (x_3 - x_4) \dots$$

and that, if it contains 5 quantities, it will become

$$p + q(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)(x_2 - x_3)(x_2 - x_4)(x_2 - x_5)(x_3 - x_4)(x_3 - x_5)(x_4 - x_5),$$

where p and q are invariant functions.

It is then shown that any rational function of five variables that takes on five different values can be written in the form

$$v = r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4,$$

where r_0, $r_1 \dots r_4$ are invariant functions, and x is one of the five variables in question.

By combining this equation with the equation

$$(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)=x^5-ax^4+bx^3-cx^2+dx-e=0,$$

we can deduce the values of x in the form

$$x=s_0+s_1v+s_2v^2+s_3v^3+s_4v^4,$$

s_0, $s_1\ldots$ being functions invariant under x_1, $x_2\ldots$ Finally, we arrive at the known theorem: *Third Theorem: If a rational function of several quantities x_1, $x_2\ldots$ has m different values, we can always find an equation of degree m whose coefficients are all functions invariant under x_1, $x_2\ldots$ and which have the m values of the function as roots; but it is impossible to find an equation of the same form of lower degree, which will have one or more of these values as roots.*

By means of the theorems established in the first three paragraphs, the author then demonstrates in the fourth that it is impossible to algebraically solve the general equation of the fifth degree.

Indeed, assuming that the general equation of the fifth degree is algebraically solvable, we can, by virtue of theorem (1), express all algebraic functions whose root is composite, by rational functions of the roots; thus, since it is impossible to express a root of a general equation by a rational function of the coefficients, it must be the case that

$$R^{\frac{1}{m}}=v,$$

where $R^{\frac{1}{m}}$ is one of the first order functions that appear in the expression of the root, R is a rational function of the coefficients of the given equation, that is, a function that is independent of the roots, and v is a rational function of the same roots. This equation yields $v^m-R=0$; and m different values of v result from interchanging the roots amongst themselves. Now the number of values of a rational function of five variables must be a divisor of the product 2.3.4.5; it follows that m, which is a prime number, must be one of the three numbers 2, 3, 5; but according to the cited theorem of Mr. Cauchy, the number 3 will be excluded, and consequently, only the values 5 and 2 remain for m.

1. If $m=5$, we will have, according to what we have seen previously,

$$v=R^{\frac{1}{5}}=r_0+r_1x+r_2x^2+r_3x^3+r_4x^4,$$

and from there

$$x=s_0+s_1R^{\frac{1}{5}}+s_2R^{\frac{2}{5}}+s_3R^{\frac{3}{5}}+s_4R^{\frac{4}{5}},$$

s_0, s_1, ... being, as well as R, functions which are invariant with respect to the roots. This value gives, according to what has been established in the second paragraph, for $s_1R^{\frac{1}{5}}$, a rational function of the roots, namely:

$$s_1R^{\frac{1}{5}} = \frac{1}{5}\left(x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^2 x_4 + \alpha x_5\right) = z,$$

where α is an imaginary root of the equation $\alpha^5 - 1 = 0$; however, this is impossible, since the right-hand side has 120 different values, while it must be a root of the equation $z^5 - s_1^5 R = 0$, which is only of degree five. The number m can therefore not be equal to 5.

2. If $m = 2$, then v will have two values which, as demonstrated by Mr. *Cauchy*, must have the form

$$v = p + qs = \sqrt{R},$$

where

$$s = (x_1 - x_2)(x_1 - x_3)\ldots(x_4 - x_5),$$

and p and q are invariant functions.

By exchanging the two roots x_1 and x_2, we have $p - qs = -\sqrt{R}$, and consequently $p = 0$, and therefore

$$\sqrt{R} = qs.$$

From there it follows that all algebraic functions of the first order that appear in the expression of the root must be of the form $\alpha + \beta\sqrt{s^2}$, where α and β are invariant functions. Now it is impossible to express a root of the general equation of the fifth degree as a function of this form; therefore, there must be, in the expression of the root, functions of the second order, which must contain a radical of the form

$$\sqrt[m]{\alpha + \beta\sqrt{s^2}} = v,$$

where β is not equal to zero; m is a prime number and v is a rational function of the roots. By changing x_1 to x_2 we have

$$\sqrt[m]{\alpha - \beta\sqrt{s^2}} = v_1,$$

which gives $vv_1 = \sqrt[m]{\alpha^2 - \beta^2 s^2}$. Now $\alpha^2 - \beta^2 s^2$ is an invariant function; therefore, if vv_1 is not also an invariant function, it must be the case that m is equal to 2. But then we would have $v = \sqrt{\alpha + \beta\sqrt{s^2}}$, which gives us four different values for v. However, this is impossible, so it must be the case that vv_1 is an invariant function. Let this function be represented by γ, then we have $v_1 = \frac{\gamma}{v}$. With this established, consider the expression

$$v + v_1 = \sqrt[m]{\alpha + \beta\sqrt{s^2}} + \frac{\gamma}{\sqrt{\alpha + \beta\sqrt{s^2}}} = p = \sqrt[m]{R} + \frac{\gamma}{\sqrt[m]{R}}.$$

This value of p may be a root of an equation of the mth degree, and since this equation will necessarily be irreducible, p will have m different values. Therefore, m must be equal to 5.

So we have

$$R^{\frac{1}{5}} + \gamma R^{-\frac{1}{5}} = r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4 = p,$$

from which we have

$$x = s_0 + s_1 p + \cdots + s_4 p^4 = t_0 + t_1 R^{\frac{1}{5}} + t_2 R^{\frac{2}{5}} + t_3 R^{\frac{3}{5}} + t_4 R^{\frac{4}{5}},$$

where t_0, $t_1 \ldots t_4$ are invariant functions. Hence we deduce, as before,

$$t_1 R^{\frac{1}{5}} = \frac{1}{5}\left(x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^2 x_4 + \alpha x_5\right) = y,$$

$$y^5 = t_1^5 R = t_1^5 \left(\alpha + \beta\sqrt{s^2}\right),$$

and

$$\left(y^5 - \alpha t_1^5\right)^2 - t_1^{10} \beta^2 s^2 = 0.$$

This equation, whose coefficients are invariant functions, is of the tenth degree with respect to y; but this contradicts theorem (3), since y has 120 different values.

We conclude therefore, in the last place, that it is impossible to algebraically solve the *general* equation of the fifth degree. From this it immediately follows that it is, in general, impossible to algebraically solve general equations of degrees greater than four.