DEMONSTRATION OF THE IMPOSSIBILITY OF AN ALGEBRAIC SOLUTION OF GENERAL EQUATIONS OF DEGREES GREATER THAN FOUR.

It is well-known that one can solve general equations of degree at most four, and equations of higher degree can be solved in some particular cases, but unless I am mistaken, no one has yet addressed the following question in a satisfactory manner: "Is it possible to solve, in general, equations of degree greater than four?". The goal of this memoire will be to answer this question.

Solving an equation algebraically means nothing more than to express its roots as algebraic functions of the coefficients. Therefore, we must first consider the general form of an algebraic function, and then determine whether or not a given equation can be satisfied by a function of this form.

I.

On the general form of algebraic functions.

Let x', x'', x''', ... be a finite number of unknown 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''', ... and other quantities which do not depend on any of these, using only the following operations: 1) addition, 2) multiplication, 3) division, and 4) extraction of roots of prime order. Here we have not included subtraction, raising to integer powers, or extraction of roots of composite order, but these are evidently combinations of the four operations we have mentioned.

When a function v can be formed using only the first three operations, it is said to be *algebraic and rational*, or simply *rational*; and if only the first two operations are required, it is said to be *algebraic, rational, and entire*, or simply *polynomial*[1].

Let $f(x', x'', x''', \dots)$ denote a general function which can be expressed as a sum of a finite number of terms

$$Ax'^{m_1}x''^{m_2}\cdots,$$

where A is a quantity which does not depend on x', x'', etc., and m_1, m_2, etc. are positive integers; it is clear that operations 1) and 2) are particular cases of the function $f(x', x'', x''', \dots)$. Therefore, a general polynomial function can be understood as the result of a limited number of repetitions of this operation. If v', v'', v''' etc. denote functions of x', x'', x''' ... which have the same general form as $f(x', x'', \dots)$, then the function $f(v', v'' \dots)$ will evidently have the same general form as $f(x', x'', \dots)$. Now $f(v', v'', \dots)$ is the general form of a function obtained from two repetitions of the operation $f(x', x'', \dots)$. We find, therefore, that the result of any number of repetitions will always take the same form. It follows that any polynomial function of $x', x'', \dots$ can be written as a sum of terms of the form $Ax'^{m_1}x''^{m_2}\cdots$.

Next we consider the rational functions. If $f(x', x'', \dots)$ and $\phi(x', x'', \dots)$ are general polynomial functions, it is clear that operations 1), 2), and 3) are particular cases of the operation

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

Therefore, a rational function can be understood as the result of repeating this operation. If v', v'', v''' are functions of the general form $\frac{f(x', x'' \dots)}{\phi(x', x'', \dots)}$, then it is easy to see that any function $\frac{f(v', v'' \dots)}{\phi(v', v'', \dots)}$ can be reduced to the same general form. It follows that any rational function of $x', x'', \dots$ can always be reduced to the form

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

where the numerator and denominator are polynomial functions.

Finally, we seek the general form of an algebraic function. If $f(x', x'', \dots)$ denotes a general rational function, it is clear that any algebraic function can be constructed with the help of

[1] We will always translate *fonction entière* as *polynomial*, in order to avoid confusion with the modern notion of an entire function.

the general operation $f(x', x'', \dots)$, combined with the operation $\sqrt[m]{r}$, where m is a prime number. Therefore, if p', p'', ... are rational functions of x', x'', ...,

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

is the general form of an algebraic function in which the operation $\sqrt[m]{r}$ is only applied to rational functions. Functions of the form p_1 will be called algebraic functions *of the first order*. Denoting by $p_1', p_1'', \dots$ any number of quantities of the form p_1, the expression

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

is the general form of an algebraic function of x', x'',..., in which the operation $\sqrt[m]{r}$ is only applied to algebraic functions of the first order. Functions of the form p_2 will be called algebraic functions *of the second order*. In the same manner, the expression

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

in which p_2', p_2'' ... are functions of the second order, will be the general form of an algebraic function of x', x'', ..., in which the operation $\sqrt[m]{r}$ is only applied to algebraic functions of the first and second order.

Continuing in this manner, one obtains algebraic functions of the third, fourth, ..., μ^{th} order, and it is clear that the expression for functions of the μ^{th} order is the *general* form of an algebraic function.

Therefore let v denote an algebraic function of order μ,

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

where p', p'', ... are functions of order $\mu - 1$; r',r'',... functions of order less than $\mu - 1$, and n', n'',... are prime numbers; f denoting, as always, a rational function of the quantities inside the parentheses.

One may evidently assume that it is impossible to express the quantities $\sqrt[n']{p'}$, $\sqrt[n'']{p''}$,... by a rational function of the quantities r', r'', ...; because otherwise, the function v would have the simpler form,

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

where the number of quantities $\sqrt[n']{p'}$, $\sqrt[n'']{p''}$ has been decreased by one. Reducing as much as possible in this way the expression for v, one either arrives at an irreducible expression, or an expression of the form

$$v = f(r', r'', r''' \dots);$$

but this function has order $\mu - 1$, contradicting the assumption that v has order μ.

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

It follows from this, that one may take

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

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

In the above discussion, we have seen that a rational function of any number of quantities may always be reduced to the form

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

where s and t are polynomial functions of the same quantities. We conclude that v can always be expressed as

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

where ϕ and τ are polynomial functions of $r', r'', \ldots$ and $\sqrt[n]{p}$. By virtue of what we have already seen, any polynomial function of the quantities s, r', r'', ... can be written 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 polynomial functions of r', r'', ... but not s. We can therefore write

$$v = \frac{t_0 + t_1 p^{\frac{1}{n}} + t_2 p^{\frac{2}{n}} + \cdots + t_m p^{\frac{m}{n}}}{v_0 + v_1 p^{\frac{1}{n}} + v_2 p^{\frac{2}{n}} + \cdots + v_m p^{\frac{m}{n}}} = \frac{T}{V}$$

where $t_0, t_1, \ldots, t_m$ and $v_0, v_1, \ldots, v_m$ are polynomial functions of r',r'',r''' etc.

Let V_1,V_2,... V_{n-1} denote the $n-1$ values of V which are found by substituting in turn $\alpha p^{\frac{1}{n}}$, $\alpha^2 p^{\frac{1}{n}}$, $\alpha^3 p^{\frac{1}{n}}$, ..., $\alpha^{n-1} p^{\frac{1}{n}}$ for $p^{\frac{1}{n}}$, where α is a root of $\alpha^n - 1$ which is not equal to 1. Multiplying the numberator and denominator of $\frac{T}{V}$ by $V_1 V_2 V_3 \cdots V_{n-1}$, one finds that

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

As one knows, the product $V V_1 V_2 \cdots V_{n-1}$ can be expressed as a polynomial function of p and the quantities r', r'' ..., and as one can see, the product $T V_1 V_2 \cdots V_{n-1}$ is a polynomial function of $\sqrt[n]{p}$ and r',r'',.... If this product is equal to

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

one finds that

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

or, writing q_0, q_1, q_2,... in place 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, q_2 are all rational functions of p, r', r'' ... etc.

If μ is any whole number, we may always write

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

where a and α are whole numbers with $\alpha < n$. It follows that

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

Putting this in place of $p^{\frac{\mu}{n}}$ 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 all rational functions of p, r', r'' ..., and consequently are functions of order μ and degree at most $m-1$, such that it is impossible to express $p^{\frac{1}{n}}$ as a rational function of these quantities.

In the expression for v above, we may always assume that $q_1 = 1$. Indeed, if q_1 is nonzero, then by setting $p_1 = p q_1^n$, one obtains

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

so

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

an expression of the same form, but with $q_1 = 1$. If instead $q_1 = 0$, let q_μ be one of the quantities $q_1, \ldots, q_{n-1}$ which is nonzero, and let $q_\mu^n p^\mu = p_1$, so that $q_\mu^\alpha p^{\frac{\alpha\mu}{n}} = p_1^{\frac{\alpha}{n}}$. Choosing whole numbers α, β, and μ', which satisfy the equation $\alpha\mu - \beta n = \mu'$, 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 remarking that $q_\mu p^{\frac{\mu}{n}} = p^{\frac{1}{n}}$, we see that v has 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 this 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,...,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 $p^{\frac{1}{n}}$ cannot be expressed as a rational function of q_0, q_1, ..., q_{n-1}.

II.

Properties of algebraic functions which satisfy a given equation.

Let

$$c_0 + c_1 y + c_2 y^2 + \cdots + c_{r-1} y^{r-1} + y^r = 0 \tag{1}$$

be an equation of degree r, where c_0, c_1,... are rational functions of the independent quantities x',x'',.... Suppose that this equation is satisfied when we replace y with an algebraic function of x', x'', ...,

$$y = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}}. \tag{2}$$

After substituting this expression for y, the proposed equation becomes, by virtue of our previous discussion, an expression of the form

$$r_0 + r_1 p^{\frac{1}{n}} + r_2 p^{\frac{2}{n}} + \cdots + r_{n-1} p^{\frac{n-1}{n}} = 0, \tag{3}$$

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

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

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

Indeed, supposing otherwise, if we set $z = p^{\frac{1}{n}}$, then the two equations

$$z^n - p = 0$$

and

$$r_0 + r_1 z + r_2 z^2 + \cdots + r_{n-1} z^n = 0,$$

will have one or more *common roots*. Letting k be the number of these roots, it is well-known that we 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

$$s_0 + s_1 z + s_2 z^2 + \cdots + s_{k-1} z^{k-1} + z^k = 0$$

be this equation, and let

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

be any factor of its left hand side, where t_0, t_1, etc. are rational functions of p, r_0, r_1,...,r_{n-1}, such that

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

We may clearly assume that it is impossible to find any equation of the same form with a smaller degree. This equation shares all of its μ roots with $z^n - p = 0$. But any root of the equation $z^n - p = 0$ takes the form αz, where α is a[n n^{th}] root of unity. Therefore, observing 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, ..., r_{n-1}, it follows that two equations must hold:

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

and

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

From these equations we get, after eliminating z^μ,

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

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

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

is irreducible, and consequently t_0 cannot be equal to zero, or we would have $\alpha^\mu-1=0$, which cannot be. Therefore,

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

Now, because of all this, it is clear that the proposed equation must be satisfied by all of the values of y obtained by assigning to $p^{\frac{1}{n}}$ all of the values $\alpha p^{\frac{1}{n}}, \alpha^2 p^{\frac{2}{n}}, \cdots \alpha^{n-1}p^{\frac{1}{n}}$. One easily sees that all of these values of y are different from one another, because otherwise there would be an equation of the form (3), and we have just seen that such an equation leads to a contradiction.

Denoting the n distinct roots of equation (1) by y_1, y_2, …, y_n, we have

$$\begin{aligned}
y_1 &= q_0+p^{\frac{1}{n}}+q_2p^{\frac{2}{n}}+\cdots+q_{n-1}p^{\frac{n-1}{n}},\\
y_2 &= q_0+\alpha p^{\frac{1}{n}}+\alpha^2q_2p^{\frac{2}{n}}+\cdots+\alpha^{n-1}q_{n-1}p^{\frac{n-1}{n}},\\
&\cdots\cdots\cdots\cdots\\
y_n &= q_0+\alpha^{n-1}p^{\frac{1}{n}}+\alpha^{n-2}q_2p^{\frac{2}{n}}+\cdots+\alpha q_{n-1}p^{\frac{n-1}{n}}.
\end{aligned}$$

Out of these n equations one can easily extract

$$\begin{aligned}
q_0 &= \frac{1}{n}\left(y_1+y_2+y_3+\cdots+y_n\right)\\
p^{\frac{1}{n}} &= \frac{1}{n}\left(y_1+\alpha^{n-1}y_2+\alpha^{n-2}y_3+\cdots+\alpha y_n\right)\\
q_2p^{\frac{2}{n}} &= \frac{1}{n}\left(y_1+\alpha^{n-2}y_2+\alpha^{n-4}y_3+\cdots+\alpha^2y_n\right)\\
&\cdots\cdots\cdots\cdots\\
q_{n-1}p^{\frac{n-1}{n}} &= \frac{1}{n}\left(y_1+\alpha y_2+\alpha^2y_3+\cdots+\alpha^{n-1}y_n\right).
\end{aligned}$$

From this one sees that the quantities $p^{\frac{1}{n}}$, q_0, q_2, …, q_{n-1} are rational functions of the roots of equation (1). Indeed, one has

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

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 that it can be solved algebraically. Let

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

by virtue of the discussion above, the quantities v, s_0, s_2 etc. can be expressed as rational functions of x_1, x_2,…,x_m, the roots of the proposed equation.

Consider one of the quantities v, s_0, s_2,…, for example v. If we denote by v_1, v_2, …, $v_{n'}$ the different values of v which are obtained by interchanging the roots x_1, x_2, …, x_m in all possible ways, we can form an equation of degree n' whose coefficients are rational functions of a, a_1,…,a_{m-1}, and whose roots are the quantities v_1,v_2,…,$v_{n'}$, which are rational functions of the quantities x_1, x_2, …, x_m.

Therefore, if we write

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

then all of the quantities $u^{\frac{1}{\nu}}$, t_0, t_2,…,$t_{\nu-1}$ will be rational functions of v_1, v_2, …, $v_{n'}$, and consequently x_1, x_2,…x_m. Treating the quantities u, t_0, t_2 etc. in a similar manner, we conclude that

If an equation can be solved algebraically, then any one of its roots can be written in such a way that the algebraic functions of which it is composed can all be expressed as rational functions of the roots of the equation.

III.

On the number of different values that a function of several quantities may acquire, when the quantities of which it is composed are exchanged amongst themselves.

Let v be a rational function of several independent quantities x_1, x_2, …, x_n. The number of different values that this function takes as we exchange the quantities on which it depends can never be greater than the product $1 \cdot 2 \cdot 3 \cdots n$. Let μ denote this product.

Let

$$v \begin{pmatrix} \alpha & \beta & \gamma & \delta & \cdots \\ a & b & c & d & \cdots \end{pmatrix}$$

denote the value taken by v when we substitute x_a, x_b, x_c, x_d, etc. for x_α, x_β, x_δ, etc. If we denote by $A_1, A_2, \ldots, A_\mu$ the μ different permutations of the indices $1, 2, 3, \ldots, n$, then it is clear that the different values of v are

$$v \begin{pmatrix} A_1 \\ A_1 \end{pmatrix} v \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} v \begin{pmatrix} A_1 \\ A_3 \end{pmatrix} \cdots v \begin{pmatrix} A_1 \\ A_\mu \end{pmatrix}$$

Suppose that the number of different values of v is less than μ. Then several of these values will be equal to v, for example

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

If we apply the substitution $v \begin{pmatrix} A_1 \\ A_{m+1} \end{pmatrix}$ to each of these quantities, we get a new series of equal values

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

which are different from the first, but equal in number. If we instead apply the substitution $v \begin{pmatrix} A_1 \\ A_{2m+1} \end{pmatrix}$, we get yet a third series of equal values, which are equal and different from the first two. Continuing this process until we have exhausted all possible permutations, the μ values of v will be partitioned into several systems, each of which contains m equal values. It follows that if ρ represents the number of different values of v, this number being equal to the number of systems, we have

$$\phi m = 1 \cdot 2 \cdot 3 \cdots n,$$

that is,

The number of different values that a function of n quantities acquires, through all possible substitutions of these quantities, is necessarily a divisor of the product $1 \cdot 2 \cdot 3 \cdots n$.

Now let $\begin{pmatrix} A_1 \\ A_m \end{pmatrix}$ be an arbitrary substitution. If we apply it several times in succession to the function v, we obtain a series of values

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

and it is clear that v necessarily must be repeated several times. When v reappears after p substitutions, we say that $\begin{pmatrix} A_1 \\ A_m \end{pmatrix}$ is a *recurrent substitution of order p*. We therefore have a periodic series,

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

or, if we write $v \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^r$ for the value of v obtained by applying the substitution $\begin{pmatrix} A_1 \\ A_m \end{pmatrix}$ a total of r times in succession, we have the series

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

It follows from this 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 suppose p be the largest prime number which is less than n. If the number of different values of v is less than p, it follows that among the following p values,

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

two of them must be equal to each other. Suppose, for example, that

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

from which one concludes that

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

Writing r in place of $r'+p-r$, and remarking that $v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{p} = v$, we have

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

where r is evidently not a multiple of p. Therefore, the value of v is neither changed by the substitution $\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{r}$, nor consequently by any number of repetitions of the same substitution. We therefore have

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

for any whole number α. But since p is a prime number, we can always find two whole numbers α and β such that

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

therefore

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

and since

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

we have

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

Therefore, the value of v is unchanged by any recurrent subsitution $\begin{pmatrix} A_1 \\ A_m \end{pmatrix}$ of order p.

Now, it is clear that both

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

are recurrent substitutions of order p, where p is the number of indices $\alpha, \beta, \gamma, \ldots, \eta$. The value of v is therefore unchanged by the combination of these two substitutions. These two substitutions are evidently equivalent to[2]

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

[2]Abel is awkwardly trying to tell us that $\begin{pmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \end{pmatrix}$ is the *composition* of two permutations of order p.

which is equivalent to the two following substitutions, applied successively:

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

Therefore,

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

and likewise

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

from which we get

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

From this we see that the function v is unchanged by two successive substitutions of the form $\begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}$, where α and β are arbitrary indices. Referring to such a substitution as a *transposition*, we can conclude that any value of v will remain unchanged by an even number of transpositions, and consequently any two values of v which result from an odd number of transpositions are equal. Any exchange of the variables of a function can be carried out with the help of 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 obtain, cannot be smaller than the largest prime number less than n, unless it is 2 or 1.

It is therefore impossible to find a function of 5 quantities which takes on 3 or 4 different values.

The proof of this theorem is taken from a memoir by *Cauchy* in the Journal de l'cole polytechnique, vol. 17.

Let v and v' be two functions, each of which has two different values. Denoting these values by v_1, v_2 and v'_1, v'_2, it follows from the above that the expressions

$$v_1 + v_2 \text{ and } v_1 v'_1 + v_2 v'_2$$

are symmetric functions. Setting

$$v_1 + v_2 = t \text{ and } v_1 v'_1 + v_2 v'_2 = t_1,$$

we have

$$v_1 = \frac{t v'_2 - t_1}{v'_2 - v'_1}.$$

When the number of quantities $x_1, x_2, \ldots, x_m$ is equal to five, the product

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

is evidently a function with two different values; its second value is the same function with the opposite sign. Therefore we may take $v'_1 = \rho$ and $v'_2 = -\rho$. The expression for v_1 then becomes

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

or equivalently

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

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

> Every function of five quantities which has two different values may be put in the form $p + q\rho$, where p and q are both symmetric functions and $\rho = (x_1 - x_2)(x_1 - x_3) \cdots (x_4 - x_5)$.

For the argument we wish to make, we will also need to know the general form taken by functions of five quantities which have five different values. This can be found as follows:

Let v be a rational function of the quantities x_1, x_2, x_3, x_4, x_5, with the property that it remains unchanged when we permute four of these quantities, say x_2,x_3,x_4,x_5. In this case, v is evidently symmetric in x_2,x_3,x_4,x_5. We may therefore express v as a rational function of x_1 and the 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 the fourth degree equation whose roots are x_2, x_3, x_4, x_5. That is, if

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

the function v may be expressed as a rational function of x_1, p, q, r, s. But if

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

then

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

from which we deduce

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

the function v may therefore be expressed as a rational function of x_1, a, b, c, d.

It follows from this that the function v can be put in the form

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

where t and ϕx_1 are polynomial functions of x_1, a, b, c, d. Multiplying the numerator and denominator by the expression $\phi x_2 \cdot \phi x_3 \cdot \phi x_4 \cdot \phi x_5$,

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

Now $\phi x_2 \cdot \phi x_3 \cdot \phi x_4 \cdot \phi x_5$ is a symmetric polynomial function of x_2, x_3, x_4, x_5. We may therefore express it as a polynomial function of p, q, r, s, and therefore as a polynomial function of x_1, a, b, c, d. The numberator of the fraction is therefore a polynomial function of the same quantities; the denominator is a symmetric function of x_1, x_2, x_3, x_4, x_5 and consequently can be expressed as a rational function of a, b, c, d, e. We can therefore write

$$v = r_0 + r_1x_1 + r_2x_2 + \cdots + r_mx_1^m,$$

[where r_0, r_1, r_2, $\ldots r_m$ are symmetric functions of a, b, c, d, e.]

Multiplying the equation

$$x_1^5 = ax_1^4 - bx_1^3 + cx_1^2 - dx_1 + e$$

successively by x_1, x_1^2, $\ldots$, x_1^{m-5}, one obtains $m-4$ equations, which can clearly be used to find expressions for x_1^5, x_1^6, $\ldots x_1^m$ of the form

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

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

On may therefore reduce v to the form

$$v = r_0 + r_1x_1 + r_2x_1^2 + r_3x_1^3 + r_4x_1^4, \tag{4}$$

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

This is the general form of a function which remains unaltered when we exchange the quantities x_2, x_3, x_4, x_5. Such a function either has 5 values, or it is symmetric.

Now let v be a rational function of x_1, x_2, x_3, x_4, x_5, which has the five values v_1, v_2, v_3, v_4, v_5. Consider the function $x_1^m v$. As we exchange the four quantities x_2, x_3, x_4, x_5 in all possible ways, the function $x_1^m v$ only takes the following values:

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

Now, I claim that the number of distinct values of $x_1^m v$ which result from these changes must be strictly less than five. Indeed, if all five values are attained, then successively exchanging x_1 with x_2, x_3, x_4, x_5 gives us 20 new values, which are necessarily different from each other and the values above. The function therefore has 25 different values, which is impossible, because 25 does not divide the product $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$. Denoting by μ the number of values taken by v when we interchange the quantities x_2, x_3, x_4, x_5 in all possible ways, we see that μ must have one of the four values 1, 2, 3, 4.

1. If $\mu = 1$, the discussion above shows that v takes the form (4).

2. If $\mu = 4$, then the sum $v_1 + v_2 + v_3 + v_4$ is a function of the form (4). But 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 $v_1+v_2+v_3+v_4$, so v_5 is of the form (4).

3. If $\mu = 2$, then $v_1 + v_2$ is a function of the form (4). Write

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

If we exchange x_1 with x_2, x_3, x_4, and x_5 in turn, we have

$$\begin{aligned} v_1 + v_2 &= \phi x_1, && (5)\\ v_2 + v_3 &= \phi x_2, && (6)\\ \cdots &\quad \cdots && (7)\\ v_{m-1} + v_m &= \phi x_{m-1}, && (8)\\ v_m + v_1 &= \phi x_m, && (9) \end{aligned}$$

where m is one of the numbers 2, 3, 4, 5. If $m = 2$, then $\phi x_1 = \phi x_2$, which is impossible, because the number of values of ϕx_1 is five. If $m = 3$, then we have

$$v_1 + v_2 = \phi x_1,\ v_2 + v_3 = \phi x_2,\ v + 3 + v_1 = \phi x_3,$$

from which we deduce

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

But the right hand side has more than 5 values, indeed it has 30. One shows in the same way that m cannot be equal to 4 or 5. It follows that μ is not equal to 2.

4. If $\mu = 3$, then $v_1 + v_2 + v_3$ has five values, and therefore so does $v_4 + v_5 = (v_1 + v_2 + v_3 + v_4 + v_5) - (v_1 + v_2 + v_3)$. But we have already seen that this is impossible. Therefore μ is also not equal to 3.

From all of this we deduce the following theorem:

> Any rational function of five quantities which has five different values necessarily takes the form
>
> $$r_0 + r_1 x + r_2 x^2 + r_x x^3 + r_4 x^4,$$
>
> where r_0, r_1, r_2 etc. are symmetric functions, and x is one of the five quantities.

From the equation

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

one can easily deduces, using the equation $x^5 - ax^4 + bx^3 - cx^2 + dx - e = 0$, an expression 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, s_3, s_4, like r_0, r_1, r_2, r_3, r_4, are symmetric functions.

Let v be a rational function which takes m different values v_1, v_2, v_3, ..., v_m. Writing

$$(v - v_1)(v - v_2)(v - v_3) \cdots (v - v_n) = q_0 + q_1 v + q_2 v^2 + \cdots + q_{m-1} v^{m-1} + v^m = 0,$$

one knows that $q_0, q_1, q_2, \ldots$ are symmetric functions, and that the m roots of the equation are v_1, v_2, v_3, ..., 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 strictly lower degree. Indeed, if

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

is such an equation, with t_0, t_1, etc. being symmetric functions, and if v_1 is a value of v which satisfies this equation, we have

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

Interchanging the variables in the function, we find the following series of equations:

$$\begin{aligned}
v^\mu + t_{\mu-1} v^{\mu-1} + \cdots &= (v - v_1) P_1 \\
v^\mu + t_{\mu-1} v^{\mu-1} + \cdots &= (v - v_2) P_2 \\
v^\mu + t_{\mu-1} v^{\mu-1} + \cdots &= (v - v_3) P_3 \\
\cdots\cdots\cdots &= \cdots \\
v^\mu + t_{\mu-1} v^{\mu-1} + \cdots &= (v - v_m) P_m
\end{aligned}$$

We conclude from this that $v - v_1$, $v - v_2$, $v - v_3$, ..., $v - v_m$ are the factors of $v^\mu + t_{\mu-1} v^{\mu-1} + \cdots$ and therefore μ is equal to m. This gives us the following theorem:

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

IV.

Demonstration of the impossibility of solving the general equation of degree five.

Using the propositions we have already shown, we can prove the theorem:

> It is impossible find a general solution of equations of degree five.

From section II, all of the algebraic functions of which an algebraic expression for one of the roots is composed can be expressed as a rational function of the roots.

Since it is impossible to express any root of an equation as a rational function of the coefficieints, we must have

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

where m is a prime number and R is a rational function of the coefficients, or equivalently a symmetric function of the roots, and v is a rational function of the roots. From this we conclude,

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

As we have seen in section II, it is impossible to lower the degree of this equation; by the final theorem of section III, v must take m different values. The number m is necessarily a divisor of $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$, so it may be equal to 2, 3, or 5. Now (see section III), no function of five variables can have three values: therefore either $m = 5$ or $m = 2$. If $m = 5$, then by the results of the previous section

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

and therefore

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

From this we deduce (see section II)

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

where $\alpha^5 = 1$. But this equation is impossible, because the right hand side has 120 values, yet it is a root of an equation of degree five, $z^5 - s_1^5 R = 0$. We therefore must have $m = 2$.

We then have (see section II),

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

where p and q are symmetric functions, and

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

Exchanging x_1 and x_2, we deduce

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

from which we see that $p = 0$ and $\sqrt{R} = qs$. We see from this that any algebraic function of the first order which can be found in the expression for the root must necessarily take the form $\alpha + \beta\sqrt{s^2} = \alpha + \beta s$, where α and β are symmetric functions. Now, it is impossible to express the root as a function of the form $\alpha + \beta\sqrt{R}$; we must therefore have 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 r is a rational function of the roots. This gives

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

where v_1 and v_2 are rational functions of the roots. Multiplying them,

$$v_1 v_2 = \sqrt[m]{\alpha^2 - \beta^2 s^2}.$$

Now $\alpha^2 - \beta^2 s^2$ is a symmetric function. If $\sqrt[m]{\alpha^2 - \beta^2 s^2}$ is not a symmetric function, then the number m, as we have seen, must be equal to 2. By in this case v would be equal to $\sqrt{\alpha + \beta\sqrt{s^2}}$, in which case it would have 4 values, which is impossible.

Therefore, it must be that $\sqrt[m]{\alpha^2 - \beta^2 s^2}$ is a symmetric function. Denoting this function by γ, we have

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

Let

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

Denote by p_1, p_2, p_3,..., p_m the different values of p which result from substituting $\alpha R^{\frac{1}{m}}$, $\alpha^2 R^{\frac{1}{m}}$, $\alpha^3 R^{\frac{1}{m}}$, ..., $\alpha^{m-1} R^{\frac{1}{m}}$ for $R^{\frac{1}{m}}$, where α satisfies

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

and consider the product

$$(p - p_1)(p - p_2) \cdots (p - p_m) = p^m - A p^{m-1} + A_1 p^{m-2} - \cdots = 0.$$

One sees easily that A, A_1 etc. are rational functions of the coefficients of the given equation, and therefore are symmetric functions of the roots. Moreover, the equation is evidently irreducible. By the final theorem of section III, it follows that p, considered as a function of the roots, must have m different values. We conclude that $m = 5$. Therefore we have

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

from which

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

or putting $\sqrt[5]{R} + \frac{\gamma}{\sqrt[5]{R}}$ in place of p,

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

where t_0, t_1, t_2 etc. are rational functions of R and the given equation. We deduce (see section II) that

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

where

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

The equation $p' = t_1 R^{\frac{1}{5}}$ implies that $p'^5 = t_1^5 R$. Since $t_1^5 R$ has the form $u + u'\sqrt{s^2}$, we have $p'^5 = u + u'\sqrt{s^2}$, which gives

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

Thus p' satisfies an equation of degree 10, whose coefficients are symmetric functions. But by the final theorem of section III this is impossible, because

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

has 120 different values. This is a contradiction.

We conclude that the general equation of degree five has no algebraic solution.

It follows immediately from this theorem that general equations of degrees greater than 5 also have no algebraic solution. Therefore, equations of degrees four and less are the only ones that can be solved algebraically in a completely general manner.