

Proof of the impossibility of solving algebraic equations of degrees higher than the fourth in general.

(By Mr. N. H. Abel.)

It is well known that one can solve algebraic equations up to the fourth degree in general, but equations of higher degrees only in particular cases, and, if I am not mistaken, the question:

Is it *possible* to solve equations of higher than the fourth degree in general? has not yet been answered satisfactorily. The present essay has this question for its subject.

To solve an equation algebraically means nothing other than to express its roots through an algebraic function of the coefficients. One must therefore first consider the general *form* of algebraic functions, and then investigate whether it is possible to satisfy the given equation in this way, namely that one sets the expression of an algebraic function in place of the unknown quantity.

§. I. On the general form of algebraic functions.

If $x', x'', x''' \dots$ are a finite set of arbitrary quantities, one says: ϱ is an algebraic function of these quantities if it can be expressed through $x', x'', x''' \dots$ etc. by means of the following operations. *First* through *addition*, *secondly* through *multiplication*, both of quantities that depend on $x', x'', x''' \dots$ and of quantities that do not depend on them; *thirdly* through *division*; fourthly through the *extraction of roots* with exponents that are prime numbers. We do not name *subtraction*, *raising to a power*, and the *extraction of roots* with composite exponents separately, because they are evidently already contained in the four operations named above.

If the function ϱ can be composed through the first three of the four operations above, it is *algebraically rational* or merely rational; and

if only the first two operations are needed, it is called *algebraically-rational* and *integral*, or also simply an *integral* function.

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

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

where A is a quantity independent of $x', x'' \dots$, and $m_1, m_2 \dots$ etc. denote whole positive numbers; then it is clear that the first two of the operations above are particular cases of the operation denoted by $f(x', x'' \dots)$. One can therefore regard *integral* functions, according to their definition, as arising from a finite number of repetitions of these operations. If one now denotes by $\varrho', \varrho'', \varrho''' \dots$ etc. several functions of the quantities $x', x'', x''' \dots$ of the same form as $f(x', x'' \dots)$, then $f(\varrho', \varrho'', \varrho''' \dots)$ is likewise evidently a function of the very same form as $f(x', x'' \dots)$. Now $f(\varrho', \varrho'' \dots)$ is the general expression of the functions that arise through a twofold repetition of the operation $f(x', x'' \dots)$. One therefore always finds the same result when one repeats the operation arbitrarily often.

From this it follows that every integral function of several quantities $x', x'' \dots$ can be expressed through the sum of several terms of the form $Ax'^{m_1}x''^{m_2} \dots$

We will now consider the rational functions.

If $f(x', x'' \dots)$ and $\varphi(x', x'' \dots)$ are two integral functions, then it is clear that the quotient

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

is a particular case of the results of the first three operations, which give rational functions. One can therefore regard a rational function as the result of the repetition of this operation. If one denotes by $\varrho', \varrho'', \varrho'''$ etc. several functions of the form $\frac{f(x', x'' \dots)}{\varphi(x', x'' \dots)}$, then it is easy to see that $\frac{f(\varrho', \varrho'' \dots)}{\varphi(\varrho', \varrho'' \dots)}$ can again be brought into the same form. It follows therefore, as above with the integral functions, that every rational function of several quantities $x', x'' \dots$ can always be brought into the form

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

where numerator and denominator are integral functions.

We will further seek the *general* form of algebraic functions.

Let one denote by $f(x', x'' \dots)$ an arbitrary rational function; then it is clear that every algebraic function can be composed by means of the operation denoted by $\sqrt[m]{r}$, combined with the operation $\sqrt[m]{r}$, where m is a prime number. If therefore $p', p'' \dots$ are rational functions of $x', x'' \dots$, then

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

will be the general form of algebraic functions of $x', x'' \dots$, in which the operation expressed by $\sqrt[m]{r}$ now refers only to rational functions. We will call the functions of the form p_1 algebraic functions of the *first order*. If one denotes by p'_1, p''_1 etc. several quantities of the form p_1 , then

$$p_2 = f(x', x'' \dots \sqrt[n']{p'}, \sqrt[n'']{p''} \dots \sqrt[n'_1]{p'_1}, \sqrt[n''_1]{p''_1} \dots)$$

will be the general form of algebraic functions of $x', x'' \dots$, in which the operation $\sqrt[m]{r}$ refers only to rational and to algebraic functions of the *first order*. We will call the functions of the form p_2 algebraic functions of the *second order*. In the same way 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 algebraic functions of $x', x'' \dots$, in which the operation $\sqrt[m]{r}$ refers only to rational and to algebraic functions of the first and second order.

If one continues in this way, one obtains algebraic functions of the *third*, *fourth* ... μ^{th} order, and it is clear that the expression of the functions of the μ^{th} order will be the *general* expression of algebraic functions.

If one therefore denotes by μ the ordinal number of an arbitrary algebraic function, and by ϱ the function itself, then

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

where $p', p'' \dots$ are functions of order $\mu - 1$; $r', r'' \dots$ functions of order $\mu - 1$, or of lower orders, and $n', n'' \dots$ are prime numbers. f denotes, as always, a rational function of the quantities standing between the brackets.

One can evidently assume that it is impossible to express one of the quantities $\sqrt[n']{p'}, \sqrt[n'']{p''} \dots$ through a rational function of the others and of the quantities $r', r'' \dots$; for were it possible, then ϱ would have the simpler form

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

in which the number of the quantities $\sqrt[n']{p'}, \sqrt[n'']{p''} \dots$ would be at least one unit smaller than above. If one now reduces this expression of ϱ still further in the same way, where feasible, then one would necessarily have to arrive at last either at an irreducible expression, or at an expression of the form

$$\varrho = f(r', r'', r''' \dots)$$

But this function would be merely of the $\mu - 1^{\text{th}}$ order, whereas ϱ should be of the μ^{th} order; which is a contradiction.

If in the expression of ϱ the number of the quantities $\sqrt[n']{p'}, \sqrt[n'']{p''} \dots$ is equal to m , then we will call the function ϱ of the μ^{th} order and of the m^{th} degree. In this way a function of the μ^{th} order and of the 0^{th} degree is the same as a function of the $\mu - 1^{\text{th}}$ order, and a function of the 0^{th} order is the same as a rational function.

From this it follows that one can set

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

where p is a function of the $\mu - 1^{\text{th}}$ order, but $r', r'' \dots$ are functions of the μ^{th} order and at most of the $m - 1^{\text{th}}$ degree, and of such a kind that it is impossible to express $\sqrt[p]{p}$ through a rational function of these quantities.

Since a rational function of several quantities, as we saw earlier, can always be brought into the form

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

where s and t are integral functions of the same variable quantities, ϱ can therefore always be expressed through

$$\varrho = \frac{\varphi(r', r'' \dots \sqrt[p]{p})}{\tau(r', r'' \dots \sqrt[p]{p})}$$

where φ and τ denote two integral functions of the quantities $r', r'' \dots$ and $\sqrt[p]{p}$. By virtue of what we found above, however, an integral function of several

quantities $s, r', r'' \dots$ can always be expressed through¹

$$t_0 + t_1 s^1 + t_2 s^2 \dots t_m s^m)$$

when $t_0, t_1 \dots t_m$ denote integral functions of $r', r'', r''' \dots$ without s . One can therefore set

$$\varrho = \frac{t_0 + t_1 p^{\frac{1}{n}} + t_2 p^{\frac{2}{n}} \dots t_m p^{\frac{m}{n}}}{\varrho_0 + \varrho_1 p^{\frac{1}{n}} + \varrho_2 p^{\frac{2}{n}} \dots \varrho_{m'} p^{\frac{m'}{n}}} = \frac{T}{V}$$

where $t_0, t_1 \dots t_m$ and $\varrho_0, \varrho_1 \dots \varrho_{m'}$ are integral functions of $r', r'', r''' \dots$ etc.

Now let $V_1, V_2 \dots V_{n-1}$ be the $n-1$ values of V that one finds when one sets $\alpha \cdot p^{\frac{1}{n}}, \alpha^2 p^{\frac{1}{n}}, \alpha^3 p^{\frac{1}{n}} \dots \alpha^{n-1} p^{\frac{1}{n}}$ in place of $p^{\frac{1}{n}}$: α denotes one of the roots of the equation $\alpha^n - 1 = 0$ that is not 1. Then one obtains, when one multiplies the fraction $\frac{T}{V}$ above and below by

$V_1 V_2 \dots V_{n-1}$ multiplied,

$$\varrho = \frac{T \cdot V_1 \cdot V_2 \dots V_{n-1}}{V \cdot V_1 \cdot V_2 \dots V_{n-1}}.$$

But the product $V \cdot V_1 \dots V_{n-1}$ can, as is well known, be expressed through an integral function of p and of the quantities $r', r'' \dots$, and the product $T \cdot V_1 \cdot V_2 \dots V_{n-1}$ is, as one sees, an integral function of $\sqrt[n]{p}$ and $r', r'' \dots$. If one therefore sets this product equal to

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

then one finds

$$\varrho = \frac{s_0 + s_1 p^{\frac{1}{n}} + s_2 p^{\frac{2}{n}} \dots s_k p^{\frac{k}{n}}}{M},$$

or, when one writes $q_0, q_1, q_2 \dots$ in place of $\frac{s_0}{m}, \frac{s_1}{m}, \frac{s_2}{m} \dots$ etc.,

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

where $q_0, q_1 \dots q_k$ are rational functions of the quantities $p, r', r'' \dots$ etc. Whatever the whole number μ may also be, one can set

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

where a and α are two whole numbers and $\alpha < n$. From this it follows that

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

If one therefore sets this expression in place of $p^{\frac{\mu}{n}}$ in the expression of ϱ , one obtains

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

¹*Editorial note:* The following display closes with a parenthesis that has no matching opening parenthesis in the print — an apparent typographical slip, reproduced here as printed.

where q_0, q_1, q_2 etc. are, as before, rational functions of $p, r', r'' \dots$ and consequently functions of the μ^{th} order and at most of the $m - 1^{\text{th}}$ degree, and of such a kind that $p^{\frac{1}{n}}$ cannot be expressed through rational functions of these quantities.

In the above expression of ϱ one can always set

$$q_1 = 1$$

For if q_1 is not zero, then one obtains, when one sets $p_1 = p \cdot q_1^n$, $p = \frac{p_1}{q_1^n}$, and $p^{\frac{1}{n}} = \frac{p_1^{\frac{1}{n}}}{q_1}$, and hence

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

which expression is of the same shape as the previous one, only that $q_1 = 1$. If $q_1 = 0$, then let q_μ be one of the quantities $q_1, q_2 \dots q_{n-1}$ that is not zero, and $q_\mu^n p^\mu = p_1$. This gives $q_\mu^\alpha \cdot p^{\frac{\alpha\mu}{n}} = p_1^{\frac{\alpha}{n}}$. If one therefore takes two whole numbers α and β that satisfy the equation $\alpha\mu - \beta n = \mu'$, where μ' is a whole number, then one obtains

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

According to this, and because $q_\mu p^{\frac{\mu}{n}} = p_1^{\frac{1}{n}}$, ϱ takes the form

$$\varrho = q_0 + p_1^{\frac{1}{n}} + q_2 p_1^{\frac{2}{n}} \dots q_{n-1} p_1^{\frac{n-1}{n}}$$

From all of this the following results:

If ϱ is an algebraic function of order μ and of degree m , then one can always set:

$$\varrho = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + q_3 p^{\frac{3}{n}} \dots q_{n-1} p^{\frac{n-1}{n}};$$

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

§. II. Properties of the algebraic functions that satisfy a given equation.

Let

$$c_0 + c_1 y + c_2 y^2 \dots + c_{r-1} y^{r-1} + y^r = 0 \quad (1)$$

be an arbitrary equation of degree r , where $c_0, c_1 \dots$ are rational functions of $x', x'' \dots$ $x', x'' \dots$ are arbitrary independent quantities. Assume that it can be satisfied when one sets in place of y some *algebraic function* of $x', x'', \dots$. Let this function be

$$y = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} \dots + q_{n-1} p^{\frac{n-1}{n}} \quad (2)$$

If one substitutes this expression of y into the given equation, then one obtains, according to the above, an expression of the form

$$r_0 + r_1 p^{\frac{1}{n}} + r_2 p^{\frac{2}{n}} \dots + r_{n-1} p^{\frac{n-1}{n}} = 0 \quad (3)$$

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

Now I assert that equation (3) cannot take place unless, individually,

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

Were this not so, then, when one denotes $p^{\frac{1}{n}}$ by z for example, the two equations

$$z^n - p = 0 \text{ and}$$

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

would have to have one or several *common roots*. Let k be the number of these roots; then one can, as is well known, find an equation that has these k roots and whose coefficients are rational functions of the quantities $p, r_0, r_1 \dots r_{n-1}$.

Let the equation be

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

and let

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

be a factor of its first term, where t_0, t_1 etc. are rational functions of $p, r_0, r_1 \dots r_{n-1}$; then likewise²

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

and it is clear that one may assume it impossible to find an equation of lower degree of the same form. This equation now has its μ roots in common with the equation $z^n - p$. But now the roots of the equation $z^n - p$ are all of the form αz , where α is some root of unity. If one therefore considers that μ cannot be smaller than 2, because it is supposed to be impossible to express z through a rational function of the quantities $p, r_0, r_1 \dots r_{n-1}$, then it follows that two equations of the form

$$\begin{aligned} t_0 + t_1 z + t_2 z^2 \dots + t_{\mu-1} z^{\mu-1} + z^\mu &= 0 \text{ and} \\ t_0 + \alpha t_1 z + \alpha^2 t_2 z^2 \dots + \alpha^{\mu-1} t_{\mu-1} z^{\mu-1} + \alpha^\mu z^\mu &= 0 \end{aligned}$$

must take place. From these equations it follows, when one eliminates z^μ ,

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

But since the equation $z^\mu + t_{\mu-1} z^{\mu-1} \dots = 0$ is irreducible, it must, because it is of the $\mu - 1^{\text{th}}$ degree, give, individually,

$$\alpha^\mu - 1 = 0, \alpha - \alpha^\mu = 0 \dots \alpha^{\mu-1} - \alpha^\mu = 0$$

² *Editorial note:* In the following display the third term is printed $t_2 z$ without an exponent; by the line just above it should read $t_2 z^2$. An apparent misprint, reproduced here as printed.

which cannot be.

It must therefore be that

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

If, however, these equations do take place, then it is clear that the given equation must be satisfied by all the values of y that one finds when one assigns to the quantity $p^{\frac{1}{n}}$ all the values $\alpha p^{\frac{1}{n}}, \alpha^2 p^{\frac{1}{n}}, \dots, \alpha^{n-1} p^{\frac{1}{n}}$.

One sees easily that all these values of y must be different from one another; for otherwise one would obtain an equation of the same shape as (3), and such an equation would, as we saw, lead to contradictions.

If one therefore denotes by $y_1, y_2 \dots y_n$ n different roots of equation (1), then one finds

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

From these n equations it easily follows that

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

One sees from this that all the quantities $p^{\frac{1}{n}}, q_0, q_2 \dots q_{n-1}$ can be expressed through rational functions of the given equation.

In fact,

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

Now take a general equation of degree m , e. g.

$$0 = a_0 + a_1 x + a_2 x^2 \dots + a_{m-1} x^{m-1} + x^m$$

and suppose it to be algebraically solvable. Let

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

then, according to the above, the quantities ϱ, s_0, s_2 etc. can be expressed through rational functions of $x_1, x_2 \dots x_m$, when one denotes by $x_1, x_2 \dots x_m$ the roots of the given equation.

Now let us examine some one of the quantities ϱ, s_0, s_2 etc., for example ϱ . Let one denote by $\varrho, \varrho_2, \dots \varrho_n$ the different values of ϱ that one finds when one interchanges the roots $x_1, x_2 \dots x_m$ among one another in every possible way; then one can set up an equation of degree n' whose coefficients are rational functions of $a_0, a_1, \dots a_{n-1}$ and whose roots are the quantities $\varrho_1, \varrho_2 \dots \varrho_{n'}$, which are rational functions of the quantities $x_1, x_2 \dots x_m$. If one therefore sets

$$\varrho = t_0 + u^{\frac{1}{\nu}} + t_2 u^{\frac{2}{\nu}} \dots + t_{\nu-1} u^{\frac{\nu-1}{\nu}}$$

then all the quantities $u^{\frac{1}{\nu}}, t_0, t_2 \dots t_{\nu-1}$ are rational functions of $\varrho_1, \varrho_2, \dots \varrho_{n'}$, and hence also of $x_1, x_2 \dots x_m$. If one proceeds in the same way with the quantities u, t_0, t_2 etc., then the following results:

If an equation is algebraically solvable, then one can always give the root such a form that all algebraic functions of which it is composed can be expressed through rational functions of the roots of the given equation.

§. III. On the number of the different values that a function of several quantities can have when the quantities on which it depends are interchanged among one another.

Let v be a rational function of several mutually independent quantities $x_1, x_2 \dots x_n$. The number of the different values of which this func-

tion is capable through interchange of the quantities on which it depends cannot be greater than the product $1 \cdot 2 \cdot 3 \dots n$. Let this product be equal to μ . 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 takes when one sets in it x_a, x_b, x_c, x_d etc. in place of $x_\alpha, x_\beta, x_\gamma, x_\delta$ etc.; then it is clear that, if one denotes by $A_1, A_2 \dots A_\mu$ the different forms of which $1, 2, 3, 4 \dots n$ are capable through interchange of the indices $1, 2, 3 \dots n$, the different values of v can be expressed through

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

Suppose that the number of the different values that v has is smaller than μ ; then several values of v must be *equal to one another*. Let then

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

If one subjects these quantities to the transformation denoted by $\begin{pmatrix} A_1 \\ A_{m+1} \end{pmatrix}$, then one obtains the 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 quantities are different from the previous ones, but equal to them in number. If one transforms these quantities anew, as is expressed by $\binom{A_1}{A_{2m+1}}$, then one obtains a new system of equal quantities, which are all different from the previous ones. If one continues in this way, until the possible transformations are exhausted, then the μ values of v will be decomposed into a certain number of systems, each of m equal values. It follows therefore that, if the number of the different values of v is equal to ϱ , which number comes out equal to the number of the systems, then

$$\varrho m = 2 \cdot 3 \cdot 4 \dots n$$

must hold, that is:

The number of the different values that a function of n quantities can obtain through the possible interchanges of these quantities is necessarily a submultiple of the product $1 \cdot 2 \cdot 3 \dots n$; as is well known.

Let now $\binom{A_1}{A_m}$ be an arbitrary transformation. Let it be carried out with v several times, so that a series of values arises

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

and it is clear that v must necessarily recur. If v returns after p transformations, then one calls $\binom{A_1}{A_m}$ a *recurring transformation of the p^{th} order*. One then has the periodic series

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

or, if one denotes by $v\binom{A_1}{A_m}^r$ the value of v that arises after the transformation denoted by $\binom{A_1}{A_m}$ has been repeated r times, the series

$$v\binom{A_1}{A_m}^0, v\binom{A_1}{A_m}^1, v\binom{A_1}{A_m}^2 \dots v\binom{A_1}{A_m}^{p-1}, v\binom{A_1}{A_m}^0 \dots$$

From this it follows that

$$v\binom{A_1}{A_m}^{\alpha p + r} = v\binom{A_1}{A_m}^r$$

$$v\binom{A_1}{A_m}^{\alpha p} = v\binom{A_1}{A_m}^0 = v.$$

Now suppose that p is the greatest prime number contained in n , and that the number of the different values of v is smaller than p ; then, among p arbitrary values of v , two must necessarily be equal to one another.

Two therefore of the p values

$$v\binom{A_1}{A_m}^0, v\binom{A_1}{A_m}^1, v\binom{A_1}{A_m}^2 \dots v\binom{A_1}{A_m}^{p-1}$$

must be equal. Let, for example,

$$v \left(\frac{A_1}{A_m} \right)^r = v \left(\frac{A_1}{A_m} \right)^{r'},$$

then it follows that

$$v \left(\frac{A_1}{A_m} \right)^{r+p-r} = v \left(\frac{A_1}{A_m} \right)^{r'+p-r}$$

This gives, because $v \left(\frac{A_1}{A_m} \right)^p = v$, when one sets r in place of $r' + p - r$,

$$v = v \left(\frac{A_1}{A_m} \right)^r;$$

where r is evidently not a multiple of p . The value of v is therefore no longer transformed by the substitution $\left(\frac{A_1}{A_m} \right)^r$, and consequently also not by the repetition of it. It is therefore

$$v = v \left(\frac{A_1}{A_m} \right)^{r\alpha},$$

where α denotes a whole number.

Now if p is a prime number, then one can evidently always find a whole number β of such a kind that

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

Therefore

$$v = v \left(\frac{A_1}{A_m} \right)^{p\beta+1},$$

or, because $v = v \left(\frac{A_1}{A_m} \right)^{p\beta}$,

$$v = v \left(\frac{A_1}{A_m} \right).$$

The value of v is therefore not changed by the *recurring* transformation $\left(\frac{A_1}{A_m} \right)$ of degree p .

Now it is clear that

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

are two *recurring* transformations of degree p , when the number of the indices $\alpha, \beta, \gamma, \dots, \eta$ is equal to p . The value of v is therefore also not changed by the combination of these two transformations. But the two transformations are evidently equivalent to the single one

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

and this single one to the two carried out one after the other

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

The value of v is therefore not changed by these two transformations combined with one another. It is 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

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

follows.

One sees from this that the function v is not changed by two successive transformations of the form $\begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}$, when α and β are two arbitrary indices. If one therefore calls such a transformation a *transposition* (transposition), then it follows that an arbitrary value of v is not changed by an even number of transpositions, and that consequently all values of v that give an odd number of transpositions are equal. But every arbitrary interchange of the elements of a function can be brought about by a certain number of transpositions: the function v can therefore have no more than two different values. This gives the following theorem:

The number of the different values of a function of n quantities can either not be diminished at all below the greatest prime number found among the factors of n , or only down to 2 or 1.

It is therefore impossible to find a function of five quantities that would have 3 or 4 different values.

The proof of this theorem is taken from a memoir by *Cauchy* that is found in the 17th cahier of the *Journal de l'école polytechnique*, page 1 etc.

Let now v and v' be two functions that each have two different values; then it is clear, according to the preceding, that if one denotes those double values by v_1, v_2 and v'_1, v'_2 , the two expressions

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

are *symmetric* functions. Let

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

then one finds

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

Now suppose that the number of the quantities $x_1, x_2 \dots x_m$ is five; then the product

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

is evidently a function that has two different values; the second

value is the same function with the opposite sign. If one therefore sets $v'_1 = \varrho$, then $v'_2 = -\varrho$. The expression of v_1 is therefore

$$v_1 = \frac{t_1 + \varrho t_2}{2\varrho}, \text{ or}$$

$$v_1 = \frac{1}{2}t_2 + \frac{t_1}{2\varrho^2}\varrho,$$

where $\frac{1}{2}t_2$ is a symmetric function. ϱ has two values that differ only in sign, so that $\frac{t_1}{2\varrho^2}$ is likewise a symmetric function. If one therefore sets $\frac{1}{2}t_2 = p$ and $\frac{t_1}{2\varrho^2} = q$, then it follows

that every function of five quantities which has two different values can be expressed through $p + q \cdot \varrho$, where p and q are two symmetric functions and

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

For our purpose we still need the general form of the functions of five quantities that have five different values. One can find them 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 one interchanges any four of the five quantities, e. g. x_2, x_3, x_4, x_5 , among one another. Under this condition v is evidently symmetric in x_2, x_3, x_4, x_5 . One can therefore express v through a rational function of x_1 and symmetric functions of x_2, x_3, x_4, x_5 . But every symmetric function of these quantities can be expressed through a rational function of the coefficients of an equation of the fourth degree whose roots are x_2, x_3, x_4, x_5 . If one therefore sets

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

then the function v can be expressed through a rational function of x_1, p, q, r, s . But if one sets

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

then one obtains

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

from which

$$p = a - x_1$$

$$q = b - ax_1 + x_1^2$$

$$r = c - bx_1 + ax_1^2 - x_1^3$$

$$s = d - cx_1 + bx_1^2 - ax_1^3 + x_1^4$$

follows. It is therefore possible to express v through a rational function of x_1, a, b, c, d and e .

From this it follows that one can bring v into the following form:

$$v = \frac{t}{\varphi(x_1)}$$

where t and $\varphi(x_1)$ are two integral functions of x_1, a, b, c, d and e . If one multiplies this fraction above and below by $\varphi(x_2), \varphi(x_3), \varphi(x_4), \varphi(x_5)$, then one finds

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

Now $\varphi(x_2) \cdot \varphi(x_3) \cdot \varphi(x_4) \cdot \varphi(x_5)$ is, as one sees, an integral and symmetric function of x_2, x_3, x_4, x_5 . One can therefore express this product through an integral function of p, q, r, s , and hence also through an integral function of x_1, a, b, c, d . The numerator of the above fraction is therefore an integral function of the same quantity; the denominator is a symmetric function of x_1, x_2, x_3, x_4, x_5 and can therefore be expressed through a rational function of a, b, c, d, e . From this it follows that one can set

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

If one multiplies the equation

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

by $x_1, x_1^2 \dots x_1^{m-5}$, then it is clear that one obtains $m - 4$ equations from which $x_1^5, x_1^6 \dots x_1^m$ can be found in turn, and indeed through quantities of the form

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

in which $\alpha, \beta, \gamma, \delta, \varepsilon$ are rational functions of a, b, c, d, e .

One can therefore bring v into the form

$$v = r_0 + r_1 x_1 + r_2 x_1^2 + r_3 x_1^3 + r_4 x_1^4 \tag{a}$$

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 the functions that do not change when one interchanges the quantities x_2, x_3, x_4, x_5 . They have either five different values, or they are symmetric.

Let now v be some 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 . Take the function $x_1^m v$:

If one interchanges in it the four quantities x_2, x_3, x_4, x_5 in every possible way, then $x_1^m v$ will each time take one of the 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 assert that the number of the values of $x_1^m v$ arising through this interchange is *smaller than five*. For if one assumes all five values, then through the interchange of x_1 with x_2, x_3, x_4, x_5 there arise from these values *twenty* others, which are necessarily different among themselves and from the previous ones. The function would thus have altogether 25 different values, which is not possible; for 25 is not a divisor of the product $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$. If one therefore denotes by μ the number of the values that v takes when one interchanges the quantities x_2, x_3, x_4, x_5 among one another, then μ must have one of the four values 1, 2, 3, 4.

1. Let $\mu = 1$; then v is, by virtue of the above, of the form (a).
2. Let $\mu = 4$; then $v_1 + v_2 + v_3 + v_4$ is a function of the form (a). But

$$v_5 = (v_1 + v_2 + v_3 + v_4 + v_5) - (v_1 + v_2 + v_3 + v_4)$$

= a *symmetric* function, less $(v_1 + v_2 + v_3 + v_4)$; hence v_5 is of the form (a).

3. Let $\mu = 2$; then $v_1 + v_2$ is a function of the form (a). Let then

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

If one interchanges x_1 in turn with x_2, x_3, x_4, x_5 , then one obtains

$$v_1 + v_2 = \varphi(x_1)$$

$$v_2 + v_3 = \varphi(x_2)$$

...

$$v_{m-1} + v_m = \varphi(x_{m-1})$$

$$v_m + v_1 = \varphi(x_m),$$

where m is one of the numbers 2, 3, 4, 5. For $m = 2$, $\varphi(x_1) = \varphi(x_2)$, which is not possible, because the number of the values of $\varphi(x_1)$ is supposed to be *five*. For $m = 3$,

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

which

$$2v_1 = \varphi(x_1) - \varphi(x_2) + \varphi(x_3)$$

gives. But the second member of this equation has more than five values, namely 30. In the same way it can be shown that m cannot be equal to 4 either. μ can therefore not be equal to two.

4. Let $\mu = 3$. Then $v_1 + v_2 + v_3$, and consequently also $v_4 + v_5 = (v_1 + v_2 + v_3 + v_4 + v_5) - (v_1 + v_2 + v_3)$, has five values. But we saw that this assumption does not take place. Therefore $\mu = 3$ cannot be the case either.

Taking all together, then, one finds the following theorem:

Every rational function of five quantities which has five different values is necessarily of the form

$$r_0 + r_1x + r_2x^2 + r_3x^3 + r_4x^4,$$

where r_0, r_1, r_2 etc. are symmetric functions, and x is one of the five quantities.

From

$$r_0 + r_1x + r_2x^2 + r_3x^3 + r_4x^4 = v$$

one easily finds, when one makes use of the given equation, the value of x expressed as follows

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

where s_0, s_1, s_2 etc. are, just like r_0, r_1, r_2 , etc., symmetric functions.

Let v be some rational function which has m different values $v_1, v_2, v_3 \dots v_m$. If one sets

$$(v - v_1)(v - v_2)(v - v_3) \dots (v - v_m) = q_0 + q_1v + q_2v^2 \dots + q_{m-1}v^{m-1} + v^m = 0,$$

then, as is well known, $q_0, q_1, q_2 \dots$ are symmetric functions, and the m roots of the equation are $v_1, v_2 \dots v_m$. Now I assert that it is impossible to express the value of v as a root of an equation of the same form but of a lower degree. For let

$$t_0 + t_1v + t_2v^2 \dots + t_{\mu-1}v^{\mu-1} + v^\mu = 0$$

be such an equation, where t_0, t_1 etc. are symmetric functions, and let v_1 be a value of v that satisfies the equation; then

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

If one now interchanges the elements of the function among one another, then one finds the following series of equations:

$$v^\mu + t_{\mu-1}v^{\mu-1} \dots = (v - v_2) \cdot P_2,$$

$$v^\mu + t_{\mu-1}v^{\mu-1} \dots = (v - v_3) \cdot P_3,$$

...

$$v^\mu + t_{\mu-1}v^{\mu-1} \dots = (v - v_m) \cdot P_m.$$

From this it follows that $v - v_1, v - v_2, v - v_3 \dots v - v_m$ are all factors

of $v^\mu + t_{\mu-1}v^{\mu-1} \dots$, and that consequently μ must necessarily be equal to m . One therefore obtains the following theorem:

If a rational function of several quantities has m different values, then one can always find an equation of degree m whose coefficients are symmetric functions and which has those values for roots; but it is not possible to set up an equation of the same form of lower degree which has one or several of those values for roots.

§. IV. Proof of the impossibility of the general solution of equations of the fifth degree.

By virtue of the propositions found above taken together, one may assert:
that it is impossible to solve equations of the fifth degree in general.

For, according to (§. II.), all algebraic functions of which an algebraic expression of the roots may be composed can be expressed through rational functions of the roots of the equation.

Since it is now impossible to express the root of an equation in general through a rational function of the coefficients, it must be that

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

where m is a prime number and R a rational function of the coefficients of the given equation, that is, a symmetric function of the roots; v is a rational function of the roots. From this it follows:

$$v^m - R = 0$$

and since, according to (§. II.), it is impossible to lower the degree of this equation, the function v will, by virtue of the last theorem in the preceding paragraph, have m different values. Since m must now be a divisor of $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$, m can be equal to 2, 3, or 5. But now, according to (§. III.), there exists no function of five quantities that has 3 values: it must therefore be that $m = 5$ or $m = 2$. Let $m = 5$; then one obtains, by virtue of the preceding paragraph,

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

and from this

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

According to (§. II.) it follows from this that

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

where $\alpha^5 = 1$. This equation is impossible, because the second member has 120 values, and yet is the root of an equation of the fifth degree $z^5 - s_1^5R = 0$.

It must therefore be that $m = 2$.

Then, according to (§. II.),

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

where p and q are symmetric functions, and

$$s = (x_1 - x_2) \dots (x_4 - x_5)$$

If one interchanges x_1 with x_2 , then

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

from which $p = 0$ and $\sqrt{R} = qs$ follow. One sees from this that all algebraic functions of the first degree found in the expression of the roots must be of the form $\alpha + \beta \cdot \sqrt{s^2} = \alpha + \beta s$, where α and β are symmetric functions. Since it is now impossible to express the roots through a function of the form $\alpha + \beta\sqrt{R}$, an equation of the form

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

must take place, where α and β are not equal to zero, m is a prime number, α and β are symmetric functions, and v is a rational function of the roots. This gives

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

where v_1 and v_2 are rational functions. If one multiplies v_2 by v_1 , then one obtains

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

Now $\alpha^2 - \beta^2 s^2$ is a symmetric function. If therefore $\sqrt[m]{(\alpha^2 - \beta^2 s^2)}$ were not a symmetric function, then, according to the above, it would have to be that $m = 2$. But then $v = \sqrt{(\alpha + \beta\sqrt{s^2})}$, and v consequently has four different values; which is not possible. It must therefore be that $\sqrt[m]{(\alpha^2 - \beta^2 s^2)}$ is a symmetric function. Let such a function be γ ; then

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

Now take the expression

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

Let one denote the values that p can take when one sets $\alpha R^{\frac{1}{m}}, \alpha^2 R^{\frac{1}{m}}, \alpha^3 R^{\frac{1}{m}} \dots \alpha^{m-1} R^{\frac{1}{m}}$ in place of $R^{\frac{1}{m}}$, where

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

by $p_1, p_2 \dots p_m$, and form the product

$$(p - p_1)(p - p_2) \dots (p - p_m) = p^m - Ap^{m-1} + A_1 p^{m-2} \dots = 0,$$

then it is easy to see that A, A_1 etc. will be rational functions of the coefficients of the given equation, hence symmetric functions of the roots. But this equation is evidently irreducible. Therefore p must, by virtue of the last theorem in the preceding paragraph, regarded as a function of the roots, have m different values. Consequently $m = 5$. But then p is of the form (a) in the preceding paragraph. Thus

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

and consequently

$$x = s_0 + s_1p + s_2p^2 + s_3p^3 + s_4p^4,$$

that is, when one sets $R^{\frac{1}{5}} + \frac{\gamma}{R}R^{\frac{4}{5}}$ in place of p ,

$$x = t_0 + t_1R^{\frac{1}{5}} + t_2R^{\frac{2}{5}} + t_3R^{\frac{3}{5}} + t_4R^{\frac{4}{5}}$$

where t_0, t_1, t_2 etc. are rational functions of R and of the coefficients of the given equation. From this it follows, by virtue of (§. II.), that

$$t_1R^{\frac{1}{5}} = x_1 + \alpha^4x_2 + \alpha^3x_3 + \alpha^2x_4 + \alpha x_5 = p,$$

where

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

Now from $p = t_1R^{\frac{1}{5}}$ it follows that $p^5 = t_1^5R$, and because t_1^5R is of the form $u + u_1\sqrt{s^2}$, $p^5 = u + u_1\sqrt{s^2}$, which

$$(p^5 - u)^2 = u_1^2s^2$$

gives. This equation gives, as one sees, p through an equation of the 10th degree whose coefficients are all symmetric functions, which, however, by virtue of the last theorem in the preceding paragraph, is not possible; for since³

$$p = x_1 + \alpha^4x_2 + \alpha^3x_3 + \alpha^2x_4 + \alpha x_5$$

p would have 120 different values; which is a contradiction.

We conclude from all of this:

that it is impossible to solve equations of the fifth degree algebraically in general.

From this it follows immediately further that it is likewise impossible to solve equations of higher than the fifth degree in general. Hence the equations that can be solved algebraically in general are only those of the first four degrees.

³*Editorial note:* In this last occurrence the coefficient of x_4 is printed α^4 ; the identical resolvent above and on p. 82 has α^2x_4 . An apparent misprint for α^2x_4 , reproduced here as printed.