

Carl Friedrich Gauss

Collected Works

Volume III

A New Proof of the Theorem That Every Polynomial in One Variable
Can Be Resolved into Real Factors of the First or Second Degree

Complete 1799 dissertation and complete second proof of 1815

Modern English translation

The historical title matter and the complete 1799 dissertation, Articles 1–24, follow, with Gauss’s ten historical footnotes and all four figures. The complete second proof, Articles 1–20 with both historical footnotes, follows with its title matter. It was presented in 1815 and published in 1816. Later Volume-III works are outside this reader. Historical references retain the source numbering.

Historical source: Carl Friedrich Gauss, *Werke*, Volume III, Göttingen, 1866; dissertation first published at Helmstedt by C. G. Fleckeisen, 1799. Originally German title matter is rendered in modern German in the German reader; the historical original is retained separately.

AI-translated into English using OpenAI GPT-6.1 Sol; AI-produced typesetting.

Translation sources and terminology

Historical text: Carl Friedrich Gauss, *Werke*, Volume III, Göttingen, 1866. These English and German texts are AI-translated from the original-language edition. The following human translations and writings are consulted for the stated terminology and usage; their running text is not reproduced. Gauss's original mathematical formulations remain controlling.

Paul Taylor; Bernard Leak. Taylor's English translation of Gauss's second proof of the fundamental theorem of algebra, with corrections by Leak, 1983. The corresponding passages of the 1815 second proof were consulted for English polynomial, divisor, degree, symmetric-function and proof terminology. Related terminology was also consulted for the 1799 dissertation, for which this is not a parallel translation. No running text from this human translation is adopted. Its later use of complex quantities does not replace Gauss's definition of imaginary quantities here. The consulted online edition identifies the translation as December 1983, its LaTeX version as August 2003, and the underlying source as last modified on 8 June 2007. Its acknowledgements credit Mark Wainwright for returning Taylor's notes and Nikita Danilov for typo corrections.
<https://www.paultaylor.eu/misc/gauss.html>

H. Maser. German translator and editor, *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik*, Berlin: Julius Springer, 1889. Related German terminology for algebraic functions, roots, divisibility, quotients and degrees; not a parallel translation of this dissertation.
<https://archive.org/details/carlfriedrichga00gausgoog>

James Caddall Morehead and Adam Miller Hildebeitel. Translators of Gauss's *General Investigations of Curved Surfaces of 1827 and 1825*, Princeton University Library, 1902; Project Gutenberg 36856, TeX edition. Related English geometrical, coordinate and infinitely small quantity terminology; not a parallel translation of the 1799 dissertation.
<https://www.gutenberg.org/ebooks/36856>

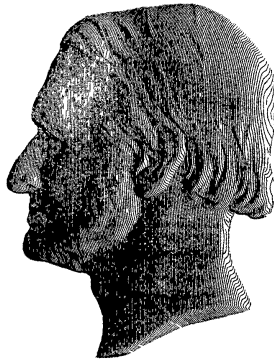
Ulrich Görtz. *Algebra*, Wintersemester 2021/22, section 3.1.1, Examples 3.1–3.2. Related contemporary German usage for polynomials, indeterminates, sums, numerators and denominators, and mathematical argument. This is a terminology reference, not a parallel translation of either proof. No running text or modern ring-theoretic argument is adopted.
<https://math.ug/a-ws2122/sect0006.html>

AI authorship and sources. AI-translated using OpenAI GPT-6.1 Sol, with AI-produced typesetting. Gauss is the author of the historical mathematical text. The named human translations are credited for their stated terminology and usage roles.

Scholarly citation metadata: CITATIONS.bib.

CARL FRIEDRICH GAUSS: WORKS
VOLUME III.

CARL FRIEDRICH GAUSS
WORKS
THIRD VOLUME



EDITED
BY THE
ROYAL SOCIETY OF SCIENCES
AT GÖTTINGEN
1866.

A NEW PROOF
OF THE THEOREM
THAT EVERY POLYNOMIAL

IN ONE VARIABLE
CAN BE RESOLVED INTO REAL FACTORS
OF THE FIRST OR SECOND DEGREE

SUBMITTED FOR
THE HIGHEST HONOURS IN PHILOSOPHY
TO THE ILLUSTRIOUS FACULTY OF PHILOSOPHY
OF THE ACADEMIA JULIA CAROLINA

BY
CARL FRIEDRICH GAUSS

HELMSTEDT
AT C. G. FLECKEISEN. MDCCLXXXIX.

A NEW PROOF OF THE THEOREM
THAT EVERY POLYNOMIAL
 IN ONE VARIABLE
 CAN BE RESOLVED INTO REAL FACTORS OF THE FIRST OR SECOND
 DEGREE.

1.

Every determinate algebraic equation can be reduced to the form

$$x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.} + M = 0$$

where m is a positive integer. If we denote the left-hand side of this equation by X and suppose that the equation $X = 0$ is satisfied by several unequal values of x , say by setting $x = \alpha$, $x = \beta$, $x = \gamma$, etc., then the function X will be divisible by the product of the factors $x - \alpha$, $x - \beta$, $x - \gamma$, etc. Conversely, if the product of several linear factors $x - \alpha$, $x - \beta$, $x - \gamma$, etc. divides the function X , then the equation $X = 0$ will be satisfied by setting x equal to any of the quantities α , β , γ , etc. Finally, if X equals a product of m such linear factors (whether they are all different or some of them are identical), no linear factors other than these can divide the function X . An equation of degree m therefore cannot have more than m roots. At the same time, however, it is evident that an equation of degree m can have *fewer* roots even if X can be resolved into m linear factors: for if some of these factors are identical, the number of different ways of satisfying the equation will necessarily be smaller than m . Yet, for the sake of uniformity, mathematicians have preferred to say that the equation has m roots in this case too, with only some of them being equal to one another; which they may certainly allow themselves to do.

2.

What has been set out so far is adequately proved in books on algebra and nowhere offends geometric rigour. But analysts seem to have adopted too hastily, and without a prior sound proof, the theorem on which almost the entire theory of equations rests: *every function such as X can always be resolved into m linear factors*, or, what agrees with this completely, *every equation of degree m actually has m roots*. Since even quadratic equations very often lead to cases that contradict this theorem, algebraists, in order to bring these cases under it, were forced to invent an imaginary quantity whose square is -1 . They then recognized that, if quantities of the form $a + b\sqrt{-1}$ are admitted in the same way as real quantities, the theorem holds not only for quadratic equations but also for cubic and biquadratic equations.

Yet this by no means justified concluding that, once quantities of the form $a + b\sqrt{-1}$ are admitted, every equation of the fifth or a higher degree can be satisfied, or, as it is usually expressed (though I would not favour this slippery wording), that the roots of every equation can be reduced to the form $a + b\sqrt{-1}$. In substance, this theorem differs in no respect from the one stated in the title of this work; giving a new rigorous proof of it is the aim of the present dissertation.

Moreover, ever since analysts discovered that there are infinitely many equations that would have no root at all unless quantities of the form $a + b\sqrt{-1}$ were admitted, such fictitious quantities have been regarded as a special kind of quantity, called *imaginary* to distinguish them from *real* quantities, and have been introduced throughout analysis. By what right? I do not discuss that here. — I shall complete my proof without any help from imaginary quantities, although I too would be entitled to use the same freedom that all recent analysts have used.

3.

Although what most elementary books offer as a proof of our theorem is so flimsy and so far removed from geometric rigour as scarcely to deserve mention, I shall nevertheless touch on it briefly so that nothing is left out. ‘To show that every equation

$$x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.} + M = 0$$

or $X = 0$ actually has m roots, they undertake to prove that X can be resolved into m linear factors. For this purpose they assume m linear factors $x - \alpha$, $x - \beta$, $x - \gamma$, etc., where α , β , γ , etc. are still unknown, and set their product equal to the function X . Then, by comparing coefficients, they obtain m equations from which, they say, the unknowns α , β , γ , etc. can be determined, since their number is also m . Namely, $m - 1$ unknowns can be eliminated, leaving an equation containing only whichever unknown one wishes.’ Passing over the other objections that could be made to such reasoning, I ask only: how can we be certain that this final equation actually has any root? Why could it not happen that no magnitude in the entire range of real and imaginary quantities satisfies either this final equation or the proposed one? — Experts will, moreover, readily see that this final equation must be *entirely identical* with the proposed one if the calculation has been carried out correctly: namely, eliminating the unknowns β , γ , etc. must give the equation

$$\alpha^m + A\alpha^{m-1} + B\alpha^{m-2} + \text{etc.} + M = 0$$

There is no need to say more about this reasoning.

Some authors who seem to have noticed the weakness of this method assume as an *axiom* that every equation actually has roots: if not possible roots, then impossible ones. They do not seem to have made sufficiently clear what they mean by possible and impossible quantities. If possible quantities are to mean the same as real quantities, and impossible quantities the same as imaginary ones, that axiom can by no means be admitted: it necessarily requires a proof. Yet the expressions do not seem intended in that sense; rather, the axiom seems to mean this: ‘Although we are not yet certain that there must be m real or imaginary quantities satisfying a given equation of degree m , we shall nevertheless suppose this for a while; for if it should happen that so many real and imaginary quantities cannot be found, we shall certainly have a way out by saying that the remaining ones are impossible.’ If someone prefers this wording to saying simply that the equation would not have so many roots in this case, I have no objection. But if he then uses these impossible roots as though they were something real, and says, for example, that the sum of all the roots of the equation $x^m + Ax^{m-1} + \text{etc.} = 0$ is $= -A$, even if there are impossible roots among them (an expression that properly means *even if some are missing*), I cannot approve of this at all. For impossible roots, understood in this sense, are still roots; that axiom therefore cannot possibly be admitted without proof, and would it be unreasonable to wonder whether there might be equations that do not even have impossible roots?*)

*)Here I always understand an imaginary quantity to mean a quantity of the form $a + b\sqrt{-1}$, as long as b is not $= 0$. All mathematicians of the first rank have always understood the expression in this sense. I do not think we should listen to those who have wished to call a quantity $a + b\sqrt{-1}$ imaginary only when $a = 0$, but impossible when $a \neq 0$ is not the case, since this distinction is neither necessary nor of any use. — If imaginary quantities are to be retained in analysis at all (which, for several reasons, seems more advisable than abolishing them, provided they are established on a sufficiently sound basis), they must necessarily be regarded as just as possible as real quantities. I would therefore prefer to include real and imaginary quantities under the common name *possible quantities*. In contrast, I would call a quantity *impossible* if it were required to satisfy conditions that cannot be satisfied even when imaginary quantities are admitted, but in such a way that this *wording* means the same as saying that no such quantity exists anywhere in the range of magnitudes. I would by no means allow a special kind of quantity to be formed from this. If someone says that a rectilinear equilateral right-angled triangle is impossible, no one will deny it. But if he wished to regard such an impossible triangle as a new kind of triangle and apply other properties of triangles to it, who could keep from laughing? This would be playing with words, or rather abusing them. — Even the greatest mathematicians have quite often applied truths that clearly presuppose the possibility of the quantities concerned to quantities whose possibility was still doubtful. Nor would I deny that such liberties generally concern only the form and, as it were, the covering of the reasoning, which a true mathematician’s sharp eye can soon penetrate. Yet it seems more advisable, and more worthy of the eminence of a science rightly celebrated as the most perfect model of clarity and certainty, either to banish such freedoms altogether, or at least to use them more sparingly and only where even the less practised can see that the matter could have been completed without their help, perhaps less briefly, but just as rigorously. — I would not, moreover, deny that what I have said here against the misuse of

4.

Before reviewing other mathematicians' proofs of our theorem and setting out what seems objectionable to me in each, I note that it is enough to show only that every equation of any degree

$$x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.} + M = 0$$

or $X = 0$ (where the coefficients A, B , etc. are supposed real) can be satisfied in at least one way by a value of x of the form $a + b\sqrt{-1}$. For it is known that X will then be divisible by the real quadratic factor $xx - 2ax + aa + bb$ if b is not $= 0$, and by the real linear factor $x - a$ if $b = 0$. In either case the quotient will be real and of lower degree than X ; and since, by the same reasoning, this quotient must have a real factor of the first or second degree, it is evident that continuing this operation will ultimately resolve the function X into real linear or quadratic factors, or, if one prefers to use two imaginary linear factors in place of each real quadratic factor, into m linear factors.

5.

The first proof of the theorem is due to the distinguished mathematician D'ALEMBERT, *Recherches sur le calcul intégral, Histoire de l'Acad. de Berlin, Année 1746*, p. 182 ff. It is also found in BOUGAINVILLE, *Traité du calcul intégral, à Paris 1754*, p. 47 ff. The principal steps of this method are as follows.

First he shows that, if any function X of the variable x becomes $= 0$ either for $x = 0$ or for $x = \infty$, and can attain an infinitely small positive real value by assigning a real value to x , this function can also attain an infinitely small negative real value through a value of x that is either real or of the imaginary form $p + q\sqrt{-1}$. Namely, if Ω denotes an infinitely small value of X , and ω the corresponding value of x , he asserts that ω can be expressed by a rapidly convergent series $a\Omega^\alpha + b\Omega^\beta + c\Omega^\gamma$, etc., where the exponents α, β, γ , etc. are continually increasing rational quantities, which therefore, at least beyond some fixed distance from the beginning, become positive and make the terms in which they occur infinitely small. Now, if none of these exponents is a fraction with an even denominator, all the terms of the series become real for both positive and negative values of Ω . If, however, there are fractions with even denominators among these exponents, then for a negative value of Ω the corresponding terms are known to have the form $p + q\sqrt{-1}$. But because of the infinite convergence of the series, in the former case it is enough to retain only the first (that is, the largest) term; in the latter there is no need to proceed beyond the term that first produces an imaginary part.

impossible quantities could in a certain respect also be objected against imaginary quantities; but I reserve their defence, together with a fuller account of this entire matter, for another occasion.

By similar reasoning it can be shown that, if X can attain an infinitely small negative value from a real value of x , this function can attain an infinitely small positive real value from a real value of x or an imaginary one of the form $p + q\sqrt{-1}$.

From this he concludes, secondly, that there is also some finite real value of X , negative in the former case and positive in the latter, that can be produced by an imaginary value of x of the form $p + q\sqrt{-1}$.

It follows that, if X is a function of x that attains a real value V from a real value v of x , and also attains from a real value of x a real value greater or smaller by an infinitely small quantity, it can also take a real value smaller or greater, respectively, than V by an infinitely small and hence by a finite quantity, by assigning to x a value of the form $p + q\sqrt{-1}$. This is readily derived from what precedes by conceiving $V + Y$ substituted for X , and $v + y$ for x .

Finally, the distinguished D'ALEMBERT asserts that, if X is supposed capable of traversing an entire interval between two real values R, S (that is, of becoming equal both to R and to S , and to all intermediate real values), by assigning to x values always of the form $p + q\sqrt{-1}$, the function X can be increased or decreased still further by any finite real quantity (according as $S > R$ or $S < R$), while x always remains of the form $p + q\sqrt{-1}$. For if there were a real quantity U (with S supposed to lie between it and R) to which X could not become equal through such a value of x , there must be a *maximum* value of X (when $S > R$; a minimum when $S < R$), say T , attained from a value $p + q\sqrt{-1}$ of x , such that no value of the same form could be assigned to x that would bring the function X any closer to U , even by the smallest amount. Now, if in this equation between X and x we substitute $p + q\sqrt{-1}$ everywhere for x and then set equal to zero both the real part and the part containing the factor $\sqrt{-1}$, after omitting that factor, two other equations can be obtained by elimination from the two resulting equations (which contain p, q and X together with constants). One contains p, X and constants; the other, free of p , contains only q, X and constants. Thus, since X has traversed all values from R to T through real values of p, q , what precedes shows that X can approach U still more closely by assigning to p, q values of the forms $\alpha + \gamma\sqrt{-1}, \beta + \delta\sqrt{-1}$, respectively. But then $x = \alpha - \delta + (\gamma + \beta)\sqrt{-1}$, that is, it is still of the form $p + q\sqrt{-1}$, contrary to the hypothesis.

Now, if X is supposed to denote a function such as $x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.} + M$, it is readily seen that real values can be assigned to x such that X traverses an entire interval between two real values. Hence x can attain some value of the form $p + q\sqrt{-1}$ from which X becomes $= 0$. Q. E. D.^{*)}

^{*)}It should be noted that, in his own account of this proof, the distinguished D'ALEMBERT used geometrical considerations, regarding X as the abscissa and x as the ordinate of a curve (following the practice of all mathematicians in the first part of this century, among whom

6.

The objections that seem possible against D'ALEMBERT's proof come down chiefly to the following.

1. The distinguished d'A. raises no doubt about the *existence* of values of x corresponding to given values of X , but assumes it and investigates only the *form* of those values.

Although this objection is in itself very serious, here it concerns only the form of expression, which can easily be corrected so as to remove it entirely.

2. The assertion that ω can always be expressed by a series of the kind he gives is certainly false if X is also to designate any transcendental function (as d'A. suggests in several places). This is evident, for example, if we put $X = e^{\frac{1}{x}}$, or $x = \frac{1}{\log X}$. Yet if we restrict the proof to the case in which X is an algebraic function of x (which suffices for the present purpose), the proposition is indeed true. — d'A., moreover, has offered nothing to support his supposition. The celebrated BOUGAINVILLE supposes X to be an algebraic function of x and recommends NEWTON's parallelogram for finding the series.

3. He uses infinitely small quantities more freely than is consistent with geometric rigour, or than a careful analyst would allow, at least in our own time (when they have a deservedly bad reputation). Nor does he make the leap from an infinitely small value of Ω to a finite one sufficiently clear. He seems to infer his proposition that Ω can also attain some finite value, less from the possibility of an infinitely small value of Ω than from this: if Ω denotes a very small quantity, then because of the rapid convergence of the series, the more terms of the series are taken, the closer one comes to the true value of ω ; or, the more terms are included in the sum taken for ω , the more accurately the equation expressing the relation between ω and Ω , or x and X , will be satisfied. Apart from the fact that this entire argument seems too vague to yield any rigorous conclusion, I note that there are indeed series that, however small a value is assigned to the quantity in whose powers they proceed, nevertheless always diverge, so that, if only they are continued far enough, one can reach terms greater than any given quantity^{*)}. This happens

the notion of functions was less familiar). Since, however, all his reasoning, considered only in its substance, rests on no geometrical principles but on purely analytical ones, and the expressions imaginary curves and imaginary ordinates seem rather harsh and more liable to offend the present-day reader, I have preferred a purely analytical presentation here. I added this note so that no one comparing D'ALEMBERT's own proof with this brief account should suspect that anything essential has been changed.

^{*)}I note in passing on this occasion that many of these series seem at first sight extremely convergent: for example, most of those that the distinguished EULER uses in the latter part of the *Inst. Calc. Diff.*, Chapter VI, pp. 441–474, to assign as closely as possible the sums of other series (the remaining series on pp. 475–478 can indeed converge). As far as I know, no one has observed this before. It would therefore be very desirable to show clearly and rigorously why series of this kind, which at first converge very rapidly, then gradually more

when the coefficients of the series form a hypergeometric progression. It was therefore necessary to prove that such a hypergeometric series could not arise in the present case.

Moreover, it seems to me that the distinguished d'A. was wrong to resort to infinite series here, and that they are unsuitable for establishing this fundamental theorem of the theory of equations.

4. From the supposition that X can attain the value S , but not the value U , it does not yet follow that between S and U there must lie a value T that X can reach but cannot exceed. Another case still remains: there could be a limit between S and U that X can approach as closely as one wishes, yet never reach. From the arguments given by the distinguished d'A. it follows only that X can exceed every value it has reached by a further finite quantity. For instance, once it has become $= S$, it can be increased by some further finite quantity Ω ; after this a new increment Ω' can be added, then another increment Ω'' , etc., so that however many increments have already been added, none should be regarded as the last, but a new one can always be added. Yet although the *number* of possible increments is bounded by no limits, it could certainly happen that, if the increments $\Omega, \Omega', \Omega''$, etc. continually decreased, the sum $S + \Omega + \Omega' + \Omega''$, etc. would nevertheless never attain some limit, however many terms were considered.

Although this case cannot occur when X denotes a polynomial in x , without a proof that it cannot happen the method must nevertheless be regarded as incomplete. When, however, X is a transcendental function, or even an algebraic fractional function, that case can indeed occur: for example, whenever an infinitely large value of x corresponds to some value of X . Then D'ALEMBERT's method seems incapable of being reduced to unquestionable principles without many complications, and perhaps in some cases not at all.

For these reasons I cannot regard D'ALEMBERT's proof as satisfactory. Nevertheless, it seems to me that its real force is by no means broken by all these objections. I believe that on the same foundation (though in a very different way, and at least with greater circumspection) not only can a rigorous proof of our theorem be built, but everything one could wish for in the theory of *transcendental* equations can be obtained from it. I shall discuss this very important matter more fully on another occasion; meanwhile, compare Article 24 below.

and more slowly, and finally diverge more and more, nevertheless give a nearly true sum provided not too many terms are taken, and how far such a sum can safely be regarded as exact?

7.

After D'ALEMBERT, the distinguished EULER published his investigations on the same subject in *Recherches sur les racines imaginaires des équations, Hist. de l'Acad. de Berlin A. 1749*, p. 223 ff. He gave two methods there; the substance of the first is as follows.

First the distinguished Euler undertakes to prove that, if m denotes any power of the number 2, the function $x^{2m} + Bx^{2m-2} + Cx^{2m-3} + \text{etc.} + M = X$ (in which the coefficient of the second term is $= 0$) can always be resolved into two real factors in which x rises to degree m . For this purpose he assumes two factors,

$$x^m - ux^{m-1} + \alpha x^{m-2} + \beta x^{m-3} + \text{etc.}, \quad \text{and} \quad x^m + ux^{m-1} + \lambda x^{m-2} + \mu x^{m-3} \text{ etc.}$$

where the coefficients u, α, β , etc., λ, μ , etc. are still unknown, and sets their product equal to the function X . Comparing coefficients then gives $2m - 1$ equations, and evidently all that must be proved is that real values satisfying these equations can be assigned to the unknowns u, α, β , etc., λ, μ , etc. (whose number is also $2m - 1$). Euler now asserts that, if u is first regarded as known, so that the number of unknowns is one less than the number of equations, then by suitably combining the equations according to known algebraic methods, all of α, β , etc., λ, μ , etc. can be determined rationally, without any extraction of roots, from u and the coefficients B, C , etc., and thus attain real values as soon as u becomes real. Moreover, all of α, β , etc., λ, μ , etc. can be eliminated to give an equation $U = 0$, where U is a polynomial in u alone and the known coefficients. Expanding this equation itself by the usual method of elimination would be an immense task when the proposed equation $X = 0$ is of a rather high degree, and completely impossible for an unspecified degree (according to Euler himself, p. 239). Yet here it is enough to know one property of this equation: the constant term in U (which does not involve the unknown u) is necessarily negative. From this it is known to follow that the equation has at least one real root, or that u , and therefore also α, β , etc., λ, μ , etc., can be determined as real quantities in at least one way. That property can be established by the following considerations. Since $x^m - ux^{m-1} + \alpha x^{m-2} + \text{etc.}$ is supposed to be a factor of the function X , u must be the sum of m roots of the equation $X = 0$, and must therefore have as many values as there are different ways of choosing m out of $2m$ roots; that is, by the principles of combinatorics, $\frac{2m \cdot 2m-1 \cdot 2m-2 \cdot \dots \cdot m+1}{1 \cdot 2 \cdot 3 \cdot \dots \cdot m}$ values. This number is always twice an odd number (I omit the proof, which is not difficult); if it is put $= 2k$, its half k is therefore odd, while the equation $U = 0$ has degree $2k$. Now, since the second term is absent in the equation $X = 0$, the sum of all $2m$ roots is 0. Thus, if the sum of any m roots is $+p$, the sum of the remaining ones is $-p$: that is, if $+p$ is among the values of u , then $-p$ is among them too. From this Euler concludes that U is the product of k quadratic factors such

as $uu - pp$, $uu - qq$, $uu - rr$, etc., where $+p$, $-p$, $+q$, $-q$, etc. denote all $2k$ roots of the equation $U = 0$. Because the number of these factors is odd, the constant term in U is therefore the square of the product pqr , etc., with a negative sign. But the product pqr , etc. can always be determined rationally from the coefficients B, C , etc., and must therefore be a real quantity. Its square with a negative sign is thus certainly a negative quantity. Q. E. D.

Since these two real factors of X have degree m , and m is a power of the number 2, each can in the same way be resolved again into two real factors of degree $\frac{1}{2}m$. Repeated halving of the number m must eventually lead to two; hence continuing the operation evidently gives the function X resolved into real quadratic factors.

If, however, a function is proposed in which the second term is not absent, say $x^{2m} + Ax^{2m-1} + Bx^{2m-2} + \text{etc.} + M$, where $2m$ still denotes a power of two, the substitution $x = y - \frac{A}{2m}$ transforms it into a similar function without a second term. It readily follows that this function too can be resolved into real quadratic factors.

Finally, given a function of degree n , where n denotes a number that is not a power of two, let the next larger power of two than n be put $= 2m$, and multiply the proposed function by any $2m - n$ real linear factors. From the fact that the product can be resolved into real quadratic factors, it readily follows that the proposed function too must be resolvable into real factors of the second or first degree.

8.

The following objections can be made to this proof.

1. The rule by which Euler concludes that all $2m - 2$ unknowns α, β , etc., λ, μ , etc. can be determined rationally from $2m - 1$ equations is by no means general, but very often admits exceptions. If, for example, in Article 3 one regards one of the unknowns as known and tries to express the others rationally in terms of it and the given coefficients, one readily finds that this is impossible, and that no unknown quantity can be determined except by an equation of degree $m - 1$. Although here one can immediately see a priori that this must necessarily happen, one might nevertheless reasonably doubt whether, in the present case too, matters stand in the same way for some values of m , so that the unknowns α, β , etc., λ, μ , etc. cannot be determined from u, B, C , etc. except by an equation of degree perhaps higher than $2m$. For the case where the equation $X = 0$ is of the fourth degree, Euler derives rational values of the coefficients in terms of u and the given coefficients; but that this can also be done for all higher equations certainly needed a fuller explanation. — It seems worthwhile, moreover, to investigate more deeply and in the greatest generality those formulas that express α, β , etc. rationally in terms of u, B, C , etc. I shall undertake a fuller treatment of this

and other matters belonging to the theory of elimination (a subject by no means exhausted) on another occasion.

2. Even if it has been proved that, whatever the degree of the equation $X = 0$, formulas can always be found that express α, β , etc., λ, μ , etc. rationally in terms of u, B, C , etc., it is nevertheless certain that for some particular values of the coefficients B, C , etc. these formulas can become *indeterminate*, so that not only is it impossible to determine these unknowns rationally from u, B, C , etc., but in some cases there are actually no real values of α, β , etc., λ, μ , etc. corresponding to a real value of u . To confirm this, for brevity I refer the reader to Euler's paper itself, where the equation of the fourth degree is discussed more fully on p. 236. Everyone will immediately see that the formulas for the coefficients α, β become indeterminate if $C = 0$ and the value 0 is taken for u , and that their values not only cannot be assigned without extracting roots, but are not even real if $BB - 4D$ is a negative quantity. Although in this case one can readily see that u has other real values to which real values of α, β correspond, one might nevertheless fear that unraveling this difficulty (which Euler did not touch on at all) could require much greater effort in higher equations. Certainly this matter must by no means be passed over in silence in an exact proof.

3. The distinguished Euler tacitly supposes that the equation $X = 0$ has $2m$ roots, and puts their sum $= 0$ because the second term is absent in X . I have already stated above, in Article 3, what I think of this freedom (which all authors on this subject use). The proposition that the sum of all the roots of an equation equals its first coefficient with its sign changed seems applicable only to equations that have roots. Since this very proof is meant to establish that the equation $X = 0$ actually has roots, it seems inadmissible to suppose their existence. No doubt those who have not yet seen through the fallacy in this reasoning will reply that *what is proved here is not that the equation $X = 0$ can be satisfied* (for that is what the expression that it has roots means), *but only that it can be satisfied by values of x contained in the form $a + b\sqrt{-1}$; the former is supposed as an axiom.* But since no forms of quantities other than the real and the imaginary $a + b\sqrt{-1}$ can be conceived, it is not sufficiently clear how what is to be proved differs from what is supposed as an axiom. Indeed, even if it were possible to devise still other forms of quantities, say the form F, F', F'' , etc., it should nevertheless not be admitted without proof that an equation can be satisfied by some value of x that is either real, or contained in the form $a + b\sqrt{-1}$, or in the form F , or in F' , etc. That axiom can therefore have no other meaning than this: any equation can be satisfied *either* by a real value of the unknown, *or* by an imaginary value contained in the form $a + b\sqrt{-1}$, *or* perhaps by a value contained in some other form hitherto unknown, *or* by a value contained in no form at all. But how quantities of this kind, of which you cannot even

form an idea — a true shadow of a shadow — can be added or multiplied is certainly not understood with the clarity always required in mathematics^{*)}.

I do not, however, wish these objections to cast any doubt on the conclusions Euler drew from his supposition. On the contrary, I am certain that they can be established by a method neither difficult nor very different from EULER'S, in such a way that not even the slightest doubt should remain for anyone. I criticize only the *form*, which, although it can be very useful in *discovering* new truths, nevertheless seems quite unacceptable in *proving* them before the public.

4. The distinguished Euler offered nothing at all to prove the assertion that the product pqr , etc. can be determined *rationally* from the coefficients in X . Everything he says about this for equations of the *fourth degree* is as follows (where a, b, c, d are the roots of the proposed equation $x^4 + Bxx + Cx + D = 0$):

‘No doubt it will be objected that I have supposed here that the quantity pqr was a real quantity and that its square $ppqqrr$ was positive; this was still doubtful, since, the roots a, b, c, d being imaginary, it could well happen that the square of the quantity pqr formed from them was negative. To this I reply that this case can never occur; for however imaginary the roots a, b, c, d may be, we nevertheless know that there must be $a + b + c + d = 0$: $ab + ac + ad + bc + bd + cd = B$; $abc + abd + acd + bcd = -C^*$; $abcd = D$, these quantities B, C, D being real. But since $p = a + b$, $q = a + c$, $r = a + d$, their product $pqr = (a + b)(a + c)(a + d)$ can be determined, *as we know*, from the quantities B, C, D , and will consequently be real, just as we have seen that in fact $pqr = -C$ and $ppqqrr = CC$. It will readily be recognized in the same way that this same circumstance must occur in higher equations, and that no objections can be made to me on this ground.’ Euler nowhere added the condition that the product pqr , etc. can be determined *rationally* in terms of B, C , etc.; nevertheless, he seems always to have understood it, since without it the proof can have no force. Now it is indeed true for equations of the fourth degree that expanding the product $(a + b)(a + c)(a + d)$ gives $aa(a + b + c + d) + abc + abd + acd + bcd = -C$; yet it does not seem sufficiently clear how in all higher equations the product can be determined rationally from the coefficients. The celebrated DE FONCENEX, who first observed this (*Miscell. phil. math. soc. Taurin.*, Vol. I, p. 117), rightly maintains that without a rigorous proof of this proposition the method loses all its

^{*)}This whole matter will be greatly clarified by another investigation already in the press, where, on a subject very different but nevertheless analogous, I could have used a similar freedom with exactly the same right as all analysts have done here with equations. Although, with the help of such fictions, I could have completed in a few words the proofs of several truths that without them became very difficult and require the most subtle devices, I nevertheless preferred to refrain from them altogether, and I hope that few would have been satisfied had I imitated the analysts' method.

^{*)}Euler has C in error, and hence also later wrongly puts $pqr = C$.

force; he confesses, however, that this proof seems rather difficult to him, and describes the path he tried in vain^{*)}. Nevertheless, the matter can be settled without much difficulty by the following method (whose substance I can only indicate here). Although in equations of the fourth degree it is not sufficiently clear that the product $(a+b)(a+c)(a+d)$ can be determined in terms of the coefficients B, C, D , one can readily see that the same product is also $= (b+a)(b+c)(b+d)$, as well as $= (c+a)(c+b)(c+d)$, and finally also $= (d+a)(d+b)(d+c)$. The product pqr will therefore be one quarter of the sum $(a+b)(a+c)(a+d) + (b+a)(b+c)(b+d) + (c+a)(c+b)(c+d) + (d+a)(d+b)(d+c)$, which, when expanded, can readily be foreseen a priori to be a polynomial in the roots a, b, c, d in which they all enter in the same way. Such functions can always be expressed rationally in terms of the coefficients of the equation whose roots are a, b, c, d . — The same thing is also evident if the product pqr is put into the form

$$\frac{1}{2}(a+b-c-d) \times \frac{1}{2}(a+c-b-d) \times \frac{1}{2}(a+d-b-c)$$

for one can readily foresee that this product, when expanded, will involve all of a, b, c, d in the same way. Those familiar with the subject will also readily gather from this how it must be applied to higher equations. — A complete account of the proof, which brevity does not allow me to include here, together with a fuller investigation of functions involving several variables in the same way, I reserve for another occasion.

I observe, moreover, that besides these four objections there are still some other points in Euler's proof that could be criticized; I pass over them in silence, however, lest I seem too severe a critic, especially since the foregoing seems sufficiently to show that the proof, at least in the form Euler proposed it, can by no means be regarded as complete.

After this proof Euler showed another way of reducing the theorem for equations whose degree is not a power of two to the solution of equations of that kind. But since this method teaches nothing for equations whose degree is a power of two, and is moreover open to all the preceding objections (except the fourth) just as the first general proof is, there is no need to discuss it more fully here.

^{*)}An error seems to have crept into this account: namely, on p. 118, line 5, instead of the symbol p ("one chose only those in which p occurred", etc.), one must necessarily read *one and the same arbitrary root of the proposed equation*, or something similar, since the former makes no sense.

9.

In the same paper, on p. 263, the distinguished Euler tried to establish our theorem in yet another way, whose substance is as follows. Given an equation $x^n + Ax^{n-1} + Bx^{n-2}$ etc. $= 0$, no analytical expression representing its roots has yet been found if the exponent $n > 4$; nevertheless it seems certain (as Euler asserts) that it can contain nothing but arithmetical operations and extractions of roots, combined more intricately the greater n is. If this is granted, Euler shows very well that, however intricately the radical signs are combined, the value of the formula can always be represented in the form $M + N\sqrt{-1}$, where M, N are real quantities.

Against this reasoning one can object that, after the efforts of so many great mathematicians, very little hope remains of ever arriving at the general solution of algebraic equations, so that it becomes more and more probable that such a solution is altogether impossible and contradictory. This should seem all the less paradoxical *since what is commonly called the solution of an equation is, strictly speaking, nothing but its reduction to pure equations*. For the solution of pure equations is not taught by this, but supposed; and if you express a root of the equation $x^m = H$ by $\sqrt[m]{H}$, you have by no means solved it, nor have you done more than if you devised some sign to denote a root of the equation $x^n + Ax^{n-1} + \text{etc.} = 0$ and put the root equal to it. It is true that pure equations far surpass all others because of the ease of finding their roots by approximation and because of the elegant connection all their roots have with one another. It is therefore by no means to be criticized that analysts have denoted their roots by a special sign. Yet from the fact that they have included this sign, just like the arithmetical signs of addition, subtraction, multiplication, division and raising to a power, under the name of *analytical expressions*, it by no means follows that a root of any equation can be represented by them. Or, putting words aside, it is supposed without sufficient reason that the solution of any equation can be reduced to the solution of pure equations. Perhaps it would not be so difficult to prove this impossibility with full rigor already for the fifth degree; I shall present my investigations on this matter more fully elsewhere. Here it is enough that the general solvability of equations, understood in that sense, is still very doubtful, and that therefore a proof whose entire force depends on that supposition carries no weight in the present state of the subject.

10.

Later, the celebrated DE FONCENEX too, having noticed a defect in EULER'S first proof (above, Article 8, objection 4) that he could not remove, tried another path and presented it on p. 120 of the paper cited^{*)}. It consists in the following.

Let an equation $Z = 0$ be proposed, where Z denotes a function of degree m in the unknown z . If m is an odd number, it is already known that this equation has a real root; if m is even, however, the celebrated Foncenex tries in the following way to prove that the equation has at least one root of the form $p + q\sqrt{-1}$. Let $m = 2^n i$, where i denotes an odd number, and suppose that $zz + uz + M$ is a divisor of the function Z . Then the individual values of u will be the sums of pairs of roots of the equation $Z = 0$, with their sign changed; hence u will have $\frac{m \cdot m - 1}{1 \cdot 2} = m'$ values. If u is supposed to be determined by an equation $U = 0$ (where U denotes a polynomial in u and the known coefficients in Z), this equation will have degree m' . One readily sees that m' will be a number of the form $2^{n-1} i'$, where i' denotes an odd number. Now, unless m' is odd, suppose again that $uu + u'u + M'$ is a divisor of U ; similar reasoning will show that u' is determined by an equation $U' = 0$, where U' is a function of degree $\frac{m' \cdot m' - 1}{1 \cdot 2}$ in u' . Putting $\frac{m' \cdot m' - 1}{1 \cdot 2} = m''$, we have that m'' is a number of the form $2^{n-2} i''$, where i'' denotes an odd number. Now, unless m'' is odd, let $u'u' + u''u' + M''$ be a divisor of the function U' ; then u'' will be determined by an equation $U'' = 0$, which, if it is supposed to have degree m''' , gives m''' as a number of the form $2^{n-3} i'''$. It is evident that in the sequence of equations $U = 0, U' = 0, U'' = 0$, etc., the one in position n will have odd degree and therefore a real root. For brevity we shall put $n = 3$, so that the equation $U'' = 0$ has a real root u'' , for one readily sees that the same reasoning holds for any other value of n . The celebrated de Foncenex then asserts that the coefficient M'' can be determined rationally from u'' and the coefficients in U' (which are readily understood to be polynomials in the coefficients in Z), or from u'' and the coefficients in Z , and is therefore real. It follows that the roots of the equation $u'u' + u''u' + M'' = 0$ will be contained in the form $p + q\sqrt{-1}$; but they will evidently satisfy the equation $U' = 0$ as well. There will therefore be some value of u' contained in the form $p + q\sqrt{-1}$. Now the coefficient M' can, in the same way as before, be determined rationally from u' and the coefficients in Z , and will therefore also be contained in the form $p + q\sqrt{-1}$. Hence the roots of the equation $uu + u'u + M' = 0$ will be contained in the same form, and will at the same time satisfy the equation $U = 0$; that is, this equation will have a root contained in the form $p + q\sqrt{-1}$. Finally, it follows from this in a similar way that M too

^{*)}The second volume of the same *Miscellanea*, p. 337, contains elucidations of this paper; these do not, however, concern the present investigation, but the logarithms of negative quantities, which had been discussed in the same paper.

is contained in the same form, as is a root of the equation $zz + uz + M = 0$, which will evidently also satisfy the proposed equation $Z = 0$. Thus any equation will have at least one root of the form $p + q\sqrt{-1}$.

11.

Objections 1, 2 and 3 that I made against EULER'S first proof (Article 8) have the same force against this method, with this difference, however: the second objection, to which EULER'S proof was open only in some special cases, must affect the present one in every case. Namely, one can prove a priori that, even if a formula is given that expresses the coefficient M' rationally in terms of u' and the coefficients in Z , this formula must necessarily become indeterminate for several values of u' ; similarly, the formula that expresses the coefficient M'' in terms of u'' becomes indeterminate for some values of u'' , etc. This is seen most clearly if we take an equation of the fourth degree as an example. Let us therefore put $m = 4$, and let the roots of the equation $Z = 0$ be $\alpha, \beta, \gamma, \delta$. Then it is evident that the equation $U = 0$ will be of the sixth degree and its roots $-(\alpha + \beta), -(\alpha + \gamma), -(\alpha + \delta), -(\beta + \gamma), -(\beta + \delta), -(\gamma + \delta)$. The equation $U' = 0$, however, will be of the fifteenth degree, and the values of u' will be

$$\begin{array}{lll} 2\alpha + \beta + \gamma, & 2\alpha + \beta + \delta, & 2\alpha + \gamma + \delta, \\ 2\beta + \alpha + \gamma, & 2\beta + \alpha + \delta, & 2\beta + \gamma + \delta, \\ 2\gamma + \alpha + \beta, & 2\gamma + \alpha + \delta, & 2\gamma + \beta + \delta, \\ 2\delta + \alpha + \beta, & 2\delta + \alpha + \gamma, & 2\delta + \beta + \gamma, \\ \alpha + \beta + \gamma + \delta, & \alpha + \beta + \gamma + \delta, & \alpha + \beta + \gamma + \delta \end{array}$$

Now we must stop at this equation, since its degree is odd, and it will in fact have the real root $\alpha + \beta + \gamma + \delta$ (which equals the first coefficient in Z with its sign changed and will therefore be not only real but also rational if the coefficients in Z are rational). But one can readily see that, if a formula is given that expresses the value of M' rationally in terms of the corresponding value of u' , it necessarily becomes indeterminate for $u' = \alpha + \beta + \gamma + \delta$. For this value will be a root of the equation $U' = 0$ *three times*, and three values of M' will correspond to it, namely $(\alpha + \beta)(\gamma + \delta)$, $(\alpha + \gamma)(\beta + \delta)$ and $(\alpha + \delta)(\beta + \gamma)$, which can all be irrational. Evidently a rational formula could in this case produce neither an irrational value of M' nor three different values. From this example one can sufficiently gather that the celebrated DE FONCENEX'S method is by no means satisfactory; if it is to be made complete in every respect, the theory of elimination must be investigated much more deeply.

12.

Finally, the distinguished LA GRANGE treated our theorem in the paper *Sur la forme des racines imaginaires des équations*, *Nouv. Mém. de l'Acad. de Berlin* 1772, p. 222 ff. This great mathematician took particular pains to supply the defects in EULER'S first proof, and in fact investigated especially those matters that constitute the second and fourth objections above (Article 8) so deeply that nothing further remains to be desired, except perhaps that some doubts seem to remain in the earlier investigation concerning the theory of elimination, on which this whole investigation rests. — Yet he did not touch on the third objection at all; indeed, the whole investigation is built on the supposition that any equation of degree m actually has m roots.

Thus, after carefully weighing what has been set out so far, I hope that those familiar with the subject will welcome a new proof of this most important theorem drawn from entirely different principles. I now proceed to give it.

13.

LEMMA. *If m denotes any positive integer, the function $\sin \varphi . x^m - \sin m\varphi . r^{m-1}x + \sin(m-1)\varphi . r^m$ will be divisible by $xx - 2 \cos \varphi . rx + rr$.*

Proof. For $m = 1$ this function becomes $= 0$ and is therefore divisible by any factor; for $m = 2$ the quotient becomes $\sin \varphi$, and for any greater value the quotient will be $\sin \varphi . x^{m-2} + \sin 2\varphi . rx^{m-3} + \sin 3\varphi . rrx^{m-4} + \text{etc.} + \sin(m-1)\varphi . r^{m-2}$. For one readily verifies that, when this function is multiplied by $xx - 2 \cos \varphi . rx + rr$, the product equals the proposed function.

14.

LEMMA. *If the quantity r and the angle φ are determined so that the equations*

$$\begin{aligned} r^m \cos m\varphi + Ar^{m-1} \cos(m-1)\varphi + Br^{m-2} \cos(m-2)\varphi + \text{etc.} \\ + Krr \cos 2\varphi + Lr \cos \varphi + M = 0 \quad . \quad . \quad [1] \\ r^m \sin m\varphi + Ar^{m-1} \sin(m-1)\varphi + Br^{m-2} \sin(m-2)\varphi + \text{etc.} \\ + Krr \sin 2\varphi + Lr \sin \varphi = 0 \quad . \quad . \quad [2] \end{aligned}$$

hold, the polynomial $x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.} + Kxx + Lx + M = X$ will be divisible by the quadratic factor $xx - 2 \cos \varphi . rx + rr$, provided we do not have $r \sin \varphi = 0$; but if $r \sin \varphi = 0$, the same polynomial will be divisible by the linear factor $x - r \cos \varphi$.

Proof. I. By the preceding article, all the following quantities will be divisible by $xx - 2 \cos \varphi \cdot rx + rr$:

$$\begin{array}{lll}
 \sin \varphi \cdot rx^m - \sin m\varphi \cdot r^m x & & + \sin(m-1)\varphi \cdot r^{m+1} \\
 A \sin \varphi \cdot rx^{m-1} - A \sin(m-1)\varphi \cdot r^{m-1} x & & + A \sin(m-2)\varphi \cdot r^m \\
 B \sin \varphi \cdot rx^{m-2} - B \sin(m-2)\varphi \cdot r^{m-2} x & & + B \sin(m-3)\varphi \cdot r^{m-1} \\
 \text{etc.} & & \text{etc.} \\
 K \sin \varphi \cdot rxx - K \sin 2\varphi \cdot rrx & & + K \sin \varphi \cdot r^3 \\
 L \sin \varphi \cdot rx - L \sin \varphi \cdot rx & & * \\
 M \sin \varphi \cdot r & * & + M \sin(-\varphi) \cdot r
 \end{array}$$

Their sum will therefore also be divisible by $xx - 2 \cos \varphi \cdot rx + rr$. Now the first parts of these quantities form the sum $\sin \varphi \cdot rX$; the second parts, added together, give 0 by [2]; and it is easy to see that the sum of the third parts also vanishes if we multiply [1] by $\sin \varphi$ and [2] by $\cos \varphi$, and subtract the former product from the latter. It follows that the polynomial $\sin \varphi \cdot rX$ is divisible by $xx - 2 \cos \varphi \cdot rx + rr$, and hence, unless $r \sin \varphi = 0$, so is the polynomial X . Q. E. P.

II. But if $r \sin \varphi = 0$, either $r = 0$ or $\sin \varphi = 0$. In the first case, $M = 0$ by [1], and thus X is divisible by x , or by $x - r \cos \varphi$; in the second case, $\cos \varphi = \pm 1$, $\cos 2\varphi = +1$, $\cos 3\varphi = \pm 1$, and in general $\cos n\varphi = \cos \varphi^n$. Thus, by [1], we obtain $X = 0$ on setting $x = r \cos \varphi$, and consequently the polynomial X will be divisible by $x - r \cos \varphi$. Q. E. S.

15.

The preceding theorem is usually proved with the aid of imaginary quantities; see EULER, *Introd. in Anal. Inf.*, Vol. I, p. 110. I thought it worth showing how it can be obtained just as easily without their aid. It is now clear that proving our theorem requires nothing more than showing the following: *Given any polynomial X of the form $x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.} + Lx + M$, r and φ can be determined so that equations [1] and [2] hold.* For it follows that X has a real factor of the first or second degree; division will necessarily produce a real quotient of lower degree, which, for the same reason, will also have a factor of the first or second degree. By continuing this operation, X will eventually be resolved into real linear or quadratic factors. The purpose of the following investigations is therefore to prove that theorem.

16.

Imagine a fixed infinite plane (the plane of the plate, Fig. 1), and in it a fixed infinite straight line GC passing through a fixed point C . Take some length as the unit, so that all lengths of straight lines can be expressed by numbers. At any point P of the plane whose distance from the centre C is r and whose angle is $GCP = \varphi$, erect a perpendicular equal to the value of the expression

$$r^m \sin m\varphi + Ar^{m-1} \sin(m-1)\varphi + \text{etc.} + Lr \sin \varphi$$

which, for brevity, I shall always denote by T in what follows. I always regard the distance r as positive; for points lying on the other side of the axis, the angle φ must be regarded either as greater than two right angles or as negative (which here amounts to the same thing). The endpoints of these perpendiculars (which must be taken above the plane for a positive value of T , below it for a negative value, and in the plane itself for a vanishing value) will lie on a continuous curved surface extending infinitely in every direction, which, for brevity, I shall call the *first surface* in what follows. In exactly the same way, refer another surface to the same plane and centre and the same axis, with its height above any point of the plane equal to

$$r^m \cos m\varphi + Ar^{m-1} \cos(m-1)\varphi + \text{etc.} + Lr \cos \varphi + M$$

an expression which, for brevity, I shall always denote by U . I shall distinguish this surface, which will likewise be continuous and extend infinitely in every direction, from the former by calling it the *second surface*. It is then clear that the whole task is to show that there is at least one point lying in the plane, in the first surface and in the second surface at the same time.

17.

It is easy to see that the first surface lies partly above and partly below the plane. For the distance r from the centre can clearly be taken so large that the remaining terms in T vanish in comparison with the first term $r^m \sin m\varphi$; and, by choosing the angle φ appropriately, this term can be made either positive or negative. The fixed plane will therefore necessarily be cut by the first surface. I shall call this intersection of the plane with the first surface the *first line*; it will thus be determined by the equation $T = 0$. For the same reason, the plane will be cut by the second surface; the intersection will form a curve determined by the equation $U = 0$, which I shall call the *second line*. Strictly speaking, each curve will consist of several branches, which may be entirely separate, though each will be a continuous line. Indeed, the first line will always be what is called a compound curve, and the axis GC must be regarded as part of this curve: whatever value is assigned to r , we always have $T = 0$ whenever $\varphi = 0$ or $= 180^\circ$. But it is better to regard the collection of all branches passing through all points where $T = 0$ as a single curve (following the usage generally accepted in higher geometry), and likewise all branches passing through all points where $U = 0$. It is now clear that the task has been reduced to showing that there is at least one point in the plane where some branch of the first line is cut by a branch of the second line. For this purpose, we must examine the nature of these lines more closely.

18.

First of all, I observe that both curves are algebraic and, when referred to orthogonal coordinates, of degree m . For if the origin of abscissas is taken at C , the abscissas x towards G , and the ordinates y towards P , we have $x = r \cos \varphi$, $y = r \sin \varphi$, and thus in general, whatever n may be,

$$\begin{aligned} r^n \sin n\varphi &= nx^{n-1}y - \frac{n \cdot n-1 \cdot n-2}{1 \cdot 2 \cdot 3}x^{n-3}y^3 \\ &\quad + \frac{n \cdot \dots \cdot n-4}{1 \cdot \dots \cdot 5}x^{n-5}y^5 - \text{etc.}, \\ r^n \cos n\varphi &= x^n - \frac{n \cdot n-1}{1 \cdot 2}x^{n-2}yy \\ &\quad + \frac{n \cdot n-1 \cdot n-2 \cdot n-3}{1 \cdot 2 \cdot 3 \cdot 4}x^{n-4}y^4 - \text{etc.} \end{aligned}$$

Both T and U will therefore consist of several terms of the form $ax^\alpha y^\beta$, where α and β denote positive integers whose sum, at its greatest, is $= m$. It can also readily be foreseen that all terms of T contain the factor y , and thus that the first line is, strictly speaking, composed of a straight line (whose equation is $y = 0$) and a curve of degree $m - 1$; but we need not take this distinction into account here.

It will be more important to investigate whether the first and second lines have arms extending to infinity, and how many and of what kind. At an infinite distance from the point C , the first line, whose equation is $\sin m\varphi + \frac{A}{r} \sin(m-1)\varphi + \frac{B}{rr} \sin(m-2)\varphi$ etc. $= 0$, will coincide with the line whose equation is $\sin m\varphi = 0$. This represents m straight lines intersecting at the point C , the first of which is the axis GCG' , while the others are inclined to it at angles of $\frac{1}{m}180^\circ$, $\frac{2}{m}180^\circ$, $\frac{3}{m}180^\circ$ etc. degrees. The first line therefore has $2m$ infinite branches, which divide the circumference of a circle drawn with infinite radius into $2m$ equal parts: the first branch cuts the circumference at the intersection of the circle and the axis, the second at a distance of $\frac{1}{m}180^\circ$, the third at a distance of $\frac{2}{m}180^\circ$, etc. In the same way, at an infinite distance from the centre the second line will have an asymptote expressed by the equation $\cos m\varphi = 0$. This is a collection of m straight lines likewise intersecting at the point C at equal angles, but in such a way that the first forms an angle of $\frac{1}{m}90^\circ$ with the axis CG , the second an angle of $\frac{3}{m}90^\circ$, the third an angle of $\frac{5}{m}90^\circ$, etc. The second line will therefore also have $2m$ infinite branches, each occupying the middle position between two neighbouring branches of the first line, so that they cut the circumference of a circle drawn with an infinitely large radius at points whose angular distances from the axis are $\frac{1}{m}90^\circ$, $\frac{3}{m}90^\circ$, $\frac{5}{m}90^\circ$, etc. It is also clear that the axis itself always forms two infinite branches of the first line, namely the first and the one in position $m + 1$. This arrangement of the branches is shown very clearly in Fig. 2,

drawn for the case $m = 4$; the branches of the second line are dotted to distinguish them from those of the first line, and the same applies to the fourth figure^{*)}. — Since these conclusions are of the greatest importance, however, and infinitely large quantities may trouble some readers, I shall also show in the next article how to obtain them without the aid of infinities.

19.

THEOREM. *With everything as above, a circle can be drawn with centre C , on whose circumference there are $2m$ points where $T = 0$ and as many where $U = 0$, arranged so that each of the latter lies between two of the former.*

Let the sum of all the coefficients A, B etc. K, L, M , taken positively, be $= S$, and take R to be both $> S\sqrt{2}$ and $> 1^*)$. I then say that what the theorem states necessarily holds for the circle drawn with radius R . For brevity, label the point of this circumference that is $\frac{1}{m}45^\circ$ from its intersection with the left part of the axis, or for which $\varphi = \frac{1}{m}45^\circ$, by (1); similarly, the point that is $\frac{3}{m}45^\circ$ from that intersection, or for which $\varphi = \frac{3}{m}45^\circ$, by (3); then the point where $\varphi = \frac{5}{m}45^\circ$ by (5), and so on up to $(8m-1)$, which is $\frac{8m-1}{m}45^\circ$ degrees from that intersection if one always proceeds in the same direction (or $\frac{1}{m}45^\circ$ in the opposite direction). Thus there are altogether $4m$ points on the circumference at equal intervals. Between $(8m-1)$ and (1) there will be one point where $T = 0$; likewise, one such point will lie between (3) and (5), between (7) and (9), between (11) and (13), etc., so that their number is $2m$. In the same way, one point where $U = 0$ will lie between (1) and (3), between (5) and (7), and between (9) and (11), so that their number is also $= 2m$. Finally, apart from these $4m$ points, there will be no others anywhere on the circumference where either T or U is $= 0$.

Proof. I. At the point (1), $m\varphi = 45^\circ$, and thus

$$T = R^{m-1}(R\sqrt{\frac{1}{2}} + A\sin(m-1)\varphi + \frac{B}{R}\sin(m-2)\varphi + \text{etc.} + \frac{L}{R^{m-2}}\sin\varphi)$$

But the sum $A\sin(m-1)\varphi + \frac{B}{R}\sin(m-2)\varphi$ etc. certainly cannot be greater than S , and must therefore be less than $R\sqrt{\frac{1}{2}}$. It follows that at this point the value of T is certainly positive. All the more, then, T will have a positive value when $m\varphi$ lies between 45° and 135° ; that is, the value of T will always be positive from the point (1) to (3). For the same reason, T will be positive everywhere from the point (9) to (11), and in general from any point $(8k+1)$ to $(8k+3)$, where k denotes any integer. Similarly, T will be negative everywhere between (5) and (7), between (13) and (15), etc., and in general between

^{*)}The fourth figure was drawn on the assumption $X = x^4 - 2xx + 3x + 10$, so that readers less accustomed to general and abstract investigations can see in a concrete case the relative positions of the two curves. The length of the line CG was taken as $= 10$ ($CN = 1,26255$.)

^{*)}When $S > \sqrt{\frac{1}{2}}$, the first condition implies the second; but when $S < \sqrt{\frac{1}{2}}$, the second implies the first.

$(8k+5)$ and $(8k+7)$; thus it cannot be $= 0$ anywhere in any of these intervals. But since its value is positive at (3) and negative at (5), it must be $= 0$ somewhere between (3) and (5); likewise somewhere between (7) and (9), between (11) and (13), etc., up to and including the interval between $(8m-1)$ and (1). Thus we have $T = 0$ at altogether $2m$ points. Q. E. P.

II. That there are no other points with this property apart from these $2m$ points is seen as follows. Since there are none between (1) and (3), between (5) and (7), etc., there could be more such points only if at least two lay in some interval between (3) and (5), or between (7) and (9), etc. Then, however, T would necessarily be a *maximum* or *minimum* somewhere in the same interval, and hence $\frac{dT}{d\varphi} = 0$. But $\frac{dT}{d\varphi} = mR^{m-2}(R \cos m\varphi + \frac{m-1}{m}A \cos(m-1)\varphi + \text{etc.})$, and between (3) and (5), $\cos m\varphi$ is always negative and $> \sqrt{\frac{1}{2}}$. It is therefore easy to see that $\frac{dT}{d\varphi}$ is negative throughout this interval; in the same way, it is positive everywhere between (7) and (9), negative between (11) and (13), etc. Thus it cannot be 0 in any of these intervals, and the supposition cannot stand. Therefore etc. Q. E. S.

III. In exactly the same way, it is proved that U has a negative value everywhere between (3) and (5), between (11) and (13), etc., and in general between $(8k+3)$ and $(8k+5)$; but a positive value between (7) and (9), between (15) and (17), etc., and in general between $(8k+7)$ and $(8k+9)$. It follows at once that $U = 0$ must hold somewhere between (1) and (3), between (5) and (7), etc., that is, at $2m$ points. But $\frac{dU}{d\varphi} = 0$ cannot hold in any of these intervals (which is easily proved in the same way as above). There will therefore be no more than those $2m$ points on the circumference of the circle where $U = 0$. Q. E. T. and Q.

The part of the theorem stating that there are no more than $2m$ points where $T = 0$, and no more than $2m$ where $U = 0$, can also be proved from the fact that equations $T = 0$, $U = 0$ represent curves of degree m . For it is known from higher geometry that such curves cannot be cut in more than $2m$ points by a circle, as a curve of the second degree.

20.

If another circle is drawn from the same centre with a radius greater than R and divided in the same way, then on this circle too there will be one point between (3) and (5) where $T = 0$, and likewise between (7) and (9), etc. It is easy to see that the less the radius of this circle differs from the radius R , the nearer such points lying between (3) and (5) on the two circumferences must be to each other. The same will hold if a circle is drawn with a radius somewhat smaller than R , but still greater than $S\sqrt{2}$ and 1. From this it is readily understood that the circumference of the circle drawn with radius R is actually *cut* by some branch of the first line at the point between (3) and (5) where $T = 0$; and the same holds for the remaining points where $T = 0$. In the

same way, it is clear that the circumference of this circle is cut by some branch of the second line at all $2m$ points where $U = 0$. These conclusions may also be expressed as follows: if a circle of the appropriate size is drawn with centre C , $2m$ branches of the first line and as many branches of the second line will enter it, in such a way that each pair of neighbouring branches of the first line is separated by some branch of the second line. See Fig. 2, where the circle will now be of finite rather than infinite size. The numbers attached to the individual branches must not be confused with the numbers by which, for brevity, I designated certain boundaries on the circumference in this and the preceding article.

21.

From this relative arrangement of the branches entering the circle, the necessary existence of an intersection of some branch of the first line with a branch of the second line inside the circle can now be deduced in so many different ways that I almost do not know which method to choose in preference to the others. The following seems the clearest. Let us label (Fig. 2) the point on the circumference where it is cut by the left part of the axis (which is itself one of the $2m$ branches of the first line) by 0; the next point, where a branch of the second line enters, by 1; the point next to this, where the second branch of the first line enters, by 2; and so on up to $4m - 1$. Thus a branch of the second line enters the circle at every point marked with an even number, while a branch of the second line enters at every point marked with an odd number. Now it is known from higher geometry that every algebraic curve (or each individual part of any algebraic curve, if it happens to consist of several parts) either returns into itself or extends to infinity in both directions. Hence, if a branch of an algebraic curve enters a bounded region, it must necessarily leave that region again somewhere^{*)}. From this it is easily concluded that every point marked with an even number (or, for

^{*)}It certainly seems to have been demonstrated well enough that an algebraic curve can neither suddenly break off anywhere (as happens, for example, with the transcendental curve whose equation is $y = \frac{1}{\log x}$), nor, after infinitely many windings, as it were lose itself at some point (like the logarithmic spiral); and, as far as I know, no one has raised a doubt on this matter. Nevertheless, if anyone demands it, I shall undertake to give a proof free from all doubt on another occasion. In the present case, however, it is clear that if some branch, for example 2, never left the circle anywhere (Fig. 3), you could enter the circle between 0 and 2, then go around the whole of this branch (which would have to lose itself in the region of the circle), and finally leave the circle again between 2 and 4, without encountering the first line anywhere along the entire path. That this is absurd is clear from the fact that, at the point where you entered the circle, the first surface was above you, and at your exit it was below you. You must therefore necessarily have encountered the first surface itself somewhere, or a point of the first line. — This reasoning, which rests on principles of the geometry of position that are no less valid than those of the geometry of magnitude, implies only that, if you enter the circle along some branch of the first line, you can leave it again at another place while always remaining on the first line; it does not imply that your path is a continuous line in the

brevity, *every even point*) must be joined within the circle to another even point by a branch of the first line; similarly, every point marked with an odd number must be joined to another such point by a branch of the second line. Although this connection of pairs of points may vary greatly with the nature of the polynomial X , so that it cannot be determined in general, it is nevertheless easy to prove that *whatever it may be, an intersection of the first line with the second line always results.*

22.

It seems that this necessity can most conveniently be proved by contradiction. Suppose, then, that each pair of even points and each pair of odd points can be joined in such a way that no intersection of a branch of the first line with a branch of the second line results. Since the axis is part of the first line, the point 0 will clearly be joined to the point $2m$. The point 1 therefore cannot be joined to any point lying beyond the axis, that is, to any point designated by a number greater than $2m$; for otherwise the joining line would necessarily cut the axis. Thus, if 1 is supposed to be joined to the point n , we shall have $n < 2m$. For a similar reason, if 2 is taken to be joined to n' , we shall have $n' < n$; for otherwise the branch $2 \dots n'$ would necessarily cut the branch $1 \dots n$. For the same reason, the point 3 will be joined to one of the points lying between 4 and n' . It is clear that if 3, 4, 5, etc. are supposed to be joined to n'' , n''' , n'''' , etc., then n''' lies between 5 and n'' , n'''' between 6 and n''' , etc. It is therefore evident that we shall eventually reach some point h joined to the point $h + 2$. Then the branch entering the circle at the point $h + 1$ will necessarily cut the branch joining the points h and $h + 2$. Since one of these two branches belongs to the first line and the other to the second, it is now clear that the supposition is contradictory, and hence that an intersection of the first line with the second line must occur somewhere. Combining this with what precedes, we conclude from all the investigations set out above that the theorem *that every polynomial in one variable can be resolved into real factors of the first or second degree* has been proved with full rigour.

23.

It is also not difficult to deduce from the same principles that there is not merely one intersection of the first line with the second, but at least m . It may, however, happen that the first line is cut by several branches of the second line at the same point, in which case the polynomial X will have several equal factors. But since it is enough here to have proved the necessity of one intersection, I shall not dwell on this further, for brevity. For the same reason, I shall not pursue other properties of these lines in more detail here:

sense accepted in higher geometry. But here it is enough for the path to be a continuous line in the ordinary sense, that is, nowhere interrupted but connected everywhere.

for example, that their intersections always occur at right angles; or that, if several arms of both curves meet at the same point, there will be as many arms of the first line as of the second, arranged alternately and intersecting at equal angles, etc.

Finally, I observe that it is by no means impossible to present the preceding proof, which I have here built on geometric principles, in a purely analytic form as well. But I thought that the presentation set out here would be less abstract, and that the true force of the proof is brought much more clearly before the eyes here than could be expected from an analytic proof.

To finish, I shall also indicate another method of proving our theorem. At first sight it will seem very different, not only from the preceding proof, but also from all the other proofs described above; yet, if one looks at its essence, it is in fact the same as D'ALEMBERT's. I leave it to the experts to compare it with his and to examine the parallel between the two; it is added solely for their sake.

24.

Above the plane of Fig. 4, I suppose the first and second surfaces to be drawn in the same way as above, relative to the axis CG and the fixed point C . Take any point on some branch of the first line, that is, where $T = 0$ (for example, any point M lying on the axis). Unless $U = 0$ holds there too, proceed from this point along the first line in the direction in which the absolute value of U decreases. If at the point M the absolute value of U happens to decrease in both directions, it is immaterial which way you proceed; I shall show at once what is to be done if U increases in both directions. It is therefore clear that, as you continue along the first line, you must eventually reach either a point where $U = 0$, or one where the value of U becomes a minimum, for example the point N . In the former case, what was sought has been found. In the latter, it can be proved that several branches of the first line intersect at this point (an even number of branches, in fact), half of which are such that, if you turn into one of them (in either direction), the value of U continues to decrease. (For brevity, I must omit the proof of this theorem, which is more lengthy than difficult.) You can therefore proceed again along this branch until U either becomes $= 0$ (as happens at P in Fig. 4) or again becomes a minimum. Then you will turn aside again, and must eventually reach a point where $U = 0$.

One might raise against this proof the doubt whether it is possible that, however far you proceed and although the value of U always decreases, these decreases nevertheless become continually slower, and that value never reaches some limit. This objection would correspond to the fourth in Article 6. But it would not be difficult to assign a boundary beyond which the value of U must not only change ever more rapidly, but can no longer *decrease*, so that the value 0 must necessarily already have occurred before you reach this boundary. I reserve for another occasion a fuller treatment of this and the remaining matters that I have only been able to indicate in this proof.

*We discovered the principles on which this proof rests at the beginning of
October 1797.*

Fig 1.

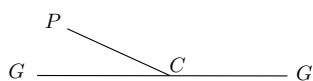


Fig.2.

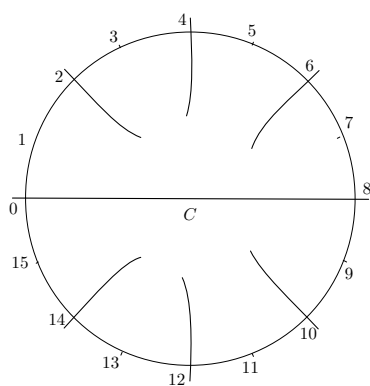


Fig 4

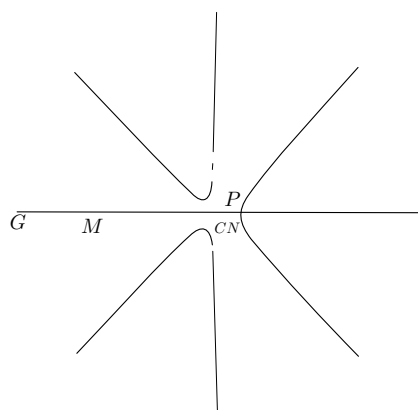
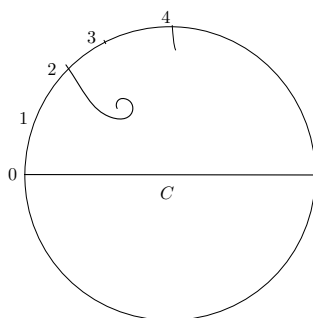


Fig 3



ANOTHER NEW PROOF
OF THE THEOREM
THAT EVERY POLYNOMIAL
IN ONE VARIABLE
CAN BE RESOLVED INTO REAL FACTORS
OF THE FIRST OR SECOND DEGREE

B Y

CARL FRIEDRICH GAUSS

**SUBMITTED TO THE ROYAL SOCIETY OF SCIENCES, 1815,
DECEMBER 7.**

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. III.

Göttingen MDCCCXVI.

**ANOTHER NEW PROOF OF THE THEOREM
THAT EVERY POLYNOMIAL
IN ONE VARIABLE
CAN BE RESOLVED INTO REAL FACTORS
OF THE FIRST OR SECOND DEGREE.**

1.

Although the proof of the theorem on resolving polynomials into factors that I gave in a paper published sixteen years ago seems to leave nothing to be desired either in rigour or in simplicity, I hope that mathematicians will not find it unwelcome if I return to this most important question and attempt to establish another proof, no less rigorous, from entirely different principles. That earlier proof depends, at least in part, on geometric considerations; the one I now undertake to set out, by contrast, will rest on purely analytic principles. In the work cited, I reviewed the more notable analytic methods by which other mathematicians had tried to prove our theorem up to that time, and gave a detailed account of the defects they suffer from. The most serious and truly fundamental of these is common to all those attempts, as well as to the more recent ones that have come to my attention; yet even then I declared that it seemed by no means unavoidable in an analytic proof. Let the experts now judge whether these further efforts have fully redeemed the pledge I gave at that time.

2.

Some preliminary investigations will precede the main discussion, both so that nothing may seem to be lacking and because their treatment may perhaps shed some fresh light even on matters that others have already touched upon. We shall first consider the greatest common divisor of two polynomials in one indeterminate. It should be stated at the outset that we are always speaking here only of polynomials: if a product is formed from two of them, each is called a *divisor* of that product. The *degree* of a divisor is determined by the exponent of the highest power of the indeterminate it contains, without any regard at all to the numerical coefficients. We can deal with the remaining matters concerning common divisors of polynomials more briefly, since they are entirely analogous to the corresponding properties of common divisors of numbers.

Given two polynomials Y, Y' in the indeterminate x , of which the former has a higher degree than the latter, or at least not a lower one, we shall form the following equations:

$$\begin{aligned} Y &= qY' + Y'' \\ Y' &= q'Y'' + Y''' \\ Y'' &= q''Y''' + Y^{(4)} \\ &\text{etc., up to} \\ Y^{(\mu-1)} &= q^{(\mu-1)}Y^{(\mu)} \end{aligned}$$

The rule is to divide Y first by Y' in the usual way; then Y' by the remainder Y'' of the first division, which has lower degree than Y' ; then again the first remainder by the second, Y''' ; and so on until a division without remainder is reached. That this must eventually happen follows from the continually decreasing degrees of the polynomials Y', Y'', Y''' etc. There is hardly any need to point out that these functions, as well as the quotients q, q', q'' etc., are *polynomials* in x . With this established, it is clear that:

I. Going backwards from the last of these equations to the first, the polynomial $Y^{(\mu)}$ is seen to divide each of the preceding ones, and is therefore certainly a common divisor of the given polynomials Y, Y' .

II. Going forwards from the first equation to the last, we see that every common divisor of the polynomials Y, Y' also divides each of the following ones, and hence the last, $Y^{(\mu)}$. Thus the polynomials Y, Y' cannot have any common divisor of higher degree than $Y^{(\mu)}$. Every common divisor of the same degree as $Y^{(\mu)}$ will stand to it in the ratio of a number to a number; hence it must itself be taken as the greatest common divisor.

III. If $Y^{(\mu)}$ has degree 0, that is, is a number, no function of the indeterminate x in the proper sense can divide Y, Y' . In this case, therefore, these polynomials are said to have no common divisor.

IV. Take the equation immediately before the last one; then eliminate $Y^{(\mu-1)}$ from it with the aid of the equation immediately before that; then again eliminate $Y^{(\mu-2)}$ with the aid of the preceding equation, and so on. In this way we obtain

$$\begin{aligned}
 Y^{(\mu)} &= +kY^{(\mu-2)} - k'Y^{(\mu-1)} \\
 &= -k'Y^{(\mu-3)} + k''Y^{(\mu-2)} \\
 &= +k''Y^{(\mu-4)} - k'''Y^{(\mu-3)} \\
 &= -k'''Y^{(\mu-5)} + k''''Y^{(\mu-4)} \\
 &\text{etc.}
 \end{aligned}$$

if we suppose the polynomials k, k', k'' etc. to be formed by the following rule:

$$\begin{aligned}
 k &= 1 \\
 k' &= q^{(\mu-2)} \\
 k'' &= q^{(\mu-3)}k' + k \\
 k''' &= q^{(\mu-4)}k'' + k' \\
 k'''' &= q^{(\mu-5)}k''' + k'' \\
 &\text{etc.}
 \end{aligned}$$

We shall therefore have

$$\pm k^{(\mu-2)}Y \mp k^{(\mu-1)}Y' = Y^{(\mu)}$$

with the upper signs applying when μ is even and the lower when it is odd. Thus, when Y and Y' have no common divisor, we can in this way find two polynomials Z, Z' in the indeterminate x such that

$$ZY + Z'Y' = 1$$

V. The converse of this proposition clearly holds as well: if the equation

$$ZY + Z'Y' = 1$$

can be satisfied with Z, Z' polynomials in the indeterminate x , then Y and Y' certainly cannot have a common divisor.

3.

The second preliminary investigation will concern the transformation of symmetric functions. Let a, b, c etc. be indeterminate quantities, m in number. Denote their sum by λ' , the sum of their products in pairs by λ'' , the sum of their products in threes by λ''' , etc., so that expanding the product

$$(x - a)(x - b)(x - c) \dots$$

gives

$$x^m - \lambda' x^{m-1} + \lambda'' x^{m-2} - \lambda''' x^{m-3} + \text{etc.}$$

Thus $\lambda', \lambda'', \lambda'''$ etc. are symmetric functions of the indeterminates a, b, c etc.: that is, functions in which these indeterminates occur in the same way, or more explicitly, functions unchanged by any permutation of these indeterminates among themselves. More generally, every polynomial in $\lambda', \lambda'', \lambda'''$ etc. (whether it contains only these indeterminates or also others independent of a, b, c etc.) will clearly be a symmetric polynomial in the indeterminates a, b, c etc.

4.

The converse theorem is somewhat less evident. Let ρ be a symmetric function of the indeterminates a, b, c etc.; it will thus consist of a certain number of terms of the form

$$Ma^{\alpha}b^{\beta}c^{\gamma} \dots$$

where α, β, γ etc. denote nonnegative integers, and M is a coefficient either fixed or at least independent of a, b, c etc. (if the function ρ happens to contain other indeterminates besides a, b, c etc.). First we shall establish a definite ordering of these individual terms. For this purpose, we first arrange the indeterminates a, b, c etc. in a definite order, which is itself entirely arbitrary: for example, with a in the first place, b in the second, c in the third, etc. Then, of the two terms

$$Ma^{\alpha}b^{\beta}c^{\gamma} \dots \quad \text{and} \quad Ma^{\alpha'}b^{\beta'}c^{\gamma'} \dots$$

we shall place the former higher in the ordering than the latter if

$$\begin{aligned} &\text{or } \alpha > \alpha', \quad \text{or } \alpha = \alpha' \text{ and } \beta > \beta', \\ &\text{or } \alpha = \alpha', \quad \beta = \beta' \text{ and } \gamma > \gamma', \quad \text{or etc.} \end{aligned}$$

that is, if the first nonvanishing one among the differences $\alpha - \alpha', \beta - \beta', \gamma - \gamma'$ etc. is positive. Terms in the same place in this ordering therefore differ only in their coefficient M , and can be combined into one term. We

shall accordingly suppose the individual terms of the function ρ to occupy different places in the ordering.

Now observe that, if $Ma^\alpha b^\beta c^\gamma \dots$ is the highest of all the terms of the function ρ in this ordering, α must be greater than, or at least not less than, β . For if $\beta > \alpha$, the term $Ma^\beta b^\alpha c^\gamma \dots$, which the function ρ must also contain since it is symmetric, would stand higher than $Ma^\alpha b^\beta c^\gamma \dots$, contrary to the hypothesis. In the same way, β will be greater than, or at least not less than, γ ; further, γ will not be less than the next exponent δ , etc. Hence each of the differences $\alpha - \beta$, $\beta - \gamma$, $\gamma - \delta$ etc. is a nonnegative integer.

Secondly, consider a product formed from any number of polynomials in the indeterminates a, b, c etc. Its highest term must be the product of the highest terms of those factors. It is equally clear that the highest terms of the functions $\lambda', \lambda'', \lambda'''$ etc. are respectively a, ab, abc etc. It follows that the highest term arising from the product

$$p = M\lambda'^{\alpha-\beta}\lambda''^{\beta-\gamma}\lambda'''^{\gamma-\delta} \dots$$

is $Ma^\alpha b^\beta c^\gamma \dots$. Thus, on setting $\rho - p = \rho'$, the highest term of the function ρ' will certainly stand lower in the ordering than the highest term of the function ρ . But p , and therefore also ρ' , are clearly symmetric polynomials in a, b, c etc. Treating ρ' in the same way as ρ before it, we can therefore split it into $p' + \rho''$, where p' is a product of powers of $\lambda', \lambda'', \lambda'''$ etc. multiplied by a coefficient either fixed or at least independent of a, b, c etc., while ρ'' is a symmetric polynomial in a, b, c etc. whose highest term stands lower in the ordering than the highest term of ρ' . Continuing in the same way, ρ will clearly at last be reduced to the form $p + p' + p'' + p'''$ etc., that is, transformed into a polynomial in $\lambda', \lambda'', \lambda'''$ etc.

5.

We can also state the theorem proved in the preceding article as follows. Given any symmetric polynomial ρ in the indeterminates a, b, c etc., we can specify a polynomial in as many other indeterminates l', l'', l''' etc. which becomes ρ under the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc. It is also easy to show that *this can be done in only one way*. For suppose that two different functions of the indeterminates l', l'', l''' etc., namely r and r' , yield the same function of a, b, c etc. after the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc. Then $r - r'$ will be a function of l', l'', l''' etc. which does not vanish in itself, but vanishes identically after those substitutions. We shall readily see that this is absurd if we consider that $r - r'$ must consist of a certain number of parts of the form

$$Ml'^\alpha l''^\beta l'''^\gamma \dots$$

whose coefficients M do not vanish and which all differ from one another in their exponents.

The highest terms arising from these individual parts are therefore given by

$$Ma^{\alpha+\beta+\gamma+\text{etc.}}b^{\beta+\gamma+\text{etc.}}c^{\gamma+\text{etc.}}\dots$$

and must consequently occupy different places in the ordering, so that the highest term of all cannot possibly cancel.

The actual calculation for transformations of this kind could, moreover, be greatly shortened by various shortcuts. We do not dwell on them here, since the mere possibility of the transformation already suffices for our purpose.

6.

Consider the product of $m(m-1)$ factors

$$\begin{aligned} &(a-b)(a-c)(a-d)\dots \\ &\times(b-a)(b-c)(b-d)\dots \\ &\times(c-a)(c-b)(c-d)\dots \\ &\times(d-a)(d-b)(d-c)\dots \\ &\text{etc.} \end{aligned}$$

which we shall denote by π . Since it involves the indeterminates a, b, c etc. symmetrically, we shall suppose it reduced to the form of a polynomial in $\lambda', \lambda'', \lambda'''$ etc. Let this polynomial become p when l', l'', l''' etc. are substituted respectively for $\lambda', \lambda'', \lambda'''$ etc. With this established, we shall call p the *determinant* of the polynomial

$$y = x^m - l'x^{m-1} + l''x^{m-2} - l'''x^{m-3} + \text{etc.}$$

Thus, for example, for $m = 2$ we have

$$p = -l'^2 + 4l''$$

Likewise, for $m = 3$ we find

$$p = -l'^2l''^2 + 4l'^3l''' + 4l''^3 - 18l'l''l''' + 27l'''^2$$

The determinant of the polynomial y is therefore a polynomial in the coefficients l', l'', l''' etc. which, under the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc., becomes the product of all the differences between pairs of the quantities a, b, c etc. In the case $m = 1$, that is, when there is only one indeterminate a and hence no differences at all, it will be convenient to take the number 1 itself as the determinant of the polynomial y .

In establishing the notion of the determinant, we had to regard the coefficients of the polynomial y as indeterminate quantities. The determinant of a polynomial with fixed coefficients,

$$Y = x^m - L'x^{m-1} + L''x^{m-2} - L'''x^{m-3} + \text{etc.}$$

will be a fixed number P , namely the value of the polynomial p for $l' = L', l'' = L'', l''' = L'''$ etc. Thus, if we suppose that Y can be resolved into linear factors,

$$Y = (x - A)(x - B)(x - C) \dots$$

or that Y arises from

$$v = (x - a)(x - b)(x - c) \dots$$

by setting $a = A, b = B, c = C$ etc., so that the same substitutions turn $\lambda', \lambda'', \lambda'''$ etc. respectively into L', L'', L''' etc., then P will clearly equal the product of the factors

$$\begin{aligned} & (A - B)(A - C)(A - D) \dots \\ & \times (B - A)(B - C)(B - D) \dots \\ & \times (C - A)(C - B)(C - D) \dots \\ & \times (D - A)(D - B)(D - C) \dots \\ & \text{etc.} \end{aligned}$$

It follows that, if $P = 0$, at least two of the quantities A, B, C etc. must be equal; conversely, if it is not the case that $P = 0$, all the quantities A, B, C etc. must be unequal. We now observe that, on setting $\frac{dY}{dx} = Y'$, or

$$\begin{aligned} Y' &= mx^{m-1} - (m-1)L'x^{m-2} + (m-2)L''x^{m-3} \\ &\quad - (m-3)L'''x^{m-4} + \text{etc.} \end{aligned}$$

we have

$$\begin{aligned} Y' &= (x - B)(x - C)(x - D) \dots \\ &\quad + (x - A)(x - C)(x - D) \dots \\ &\quad + (x - A)(x - B)(x - D) \dots \\ &\quad + (x - A)(x - B)(x - C) \dots \\ &\quad + \text{etc.} \end{aligned}$$

Thus, if two of the quantities A, B, C etc. are equal, for example $A = B$, then Y' will be divisible by $x - A$; in other words, Y and Y' will have the common divisor $x - A$. Conversely, if Y' is supposed to have any common divisor with Y , then Y' must contain one of the linear factors $x - A, x - B, x - C$ etc., for example the first, $x - A$. This clearly cannot happen unless A equals one of the remaining quantities B, C, D etc. From all this we therefore obtain two THEOREMS:

I. *If the determinant of the polynomial Y is $= 0$, then Y certainly has a common divisor with Y' ; hence, if Y and Y' have no common divisor, the determinant of the polynomial Y cannot be $= 0$.*

II. *If the determinant of the polynomial Y is not $= 0$, then Y and Y' certainly cannot have a common divisor; or, if Y and Y' have a common divisor, the determinant of the polynomial Y must necessarily be $= 0$.*

7.

But it must be carefully noted that the whole force of this very simple proof rests on the supposition that the polynomial Y can be resolved into linear factors. At this very point, where the general possibility of such a resolution is to be proved, that supposition would be nothing but begging the question. Yet not all those who have attempted analytic proofs of the main theorem have guarded against fallacies exactly like this. We have already pointed out the origin of this plausible illusion in the very statement of the inquiry: all of them investigated only the *form* of the roots of equations, whereas they ought to have proved their *existence*, which they rashly assumed. But enough has already been said in the paper cited above about this way of proceeding, which departs too far from rigour and clarity. We shall therefore now place the theorems of the preceding article, at least one of which we cannot do without for our purpose, on a firmer foundation. We shall begin with the second, as the easier one.

8.

Denote by ρ the function

$$\begin{aligned} & \frac{\pi(x-b)(x-c)(x-d) \dots}{(a-b)^2(a-c)^2(a-d)^2 \dots} \\ & + \frac{\pi(x-a)(x-c)(x-d) \dots}{(b-a)^2(b-c)^2(b-d)^2 \dots} \\ & + \frac{\pi(x-a)(x-b)(x-d) \dots}{(c-a)^2(c-b)^2(c-d)^2 \dots} \\ & + \frac{\pi(x-a)(x-b)(x-c) \dots}{(d-a)^2(d-b)^2(d-c)^2 \dots} \\ & + \text{etc.} \end{aligned}$$

which, since π is divisible by each denominator, is a polynomial in the indeterminates x, a, b, c etc. Further, set $\frac{dv}{dx} = v'$, so that we have

$$\begin{aligned} v' &= (x-b)(x-c)(x-d) \dots \\ &+ (x-a)(x-c)(x-d) \dots \\ &+ (x-a)(x-b)(x-d) \dots \\ &+ (x-a)(x-b)(x-c) \dots \\ &+ \text{etc.} \end{aligned}$$

For $x = a$ we clearly have $\rho v' = \pi$. Hence we conclude that the polynomial $\pi - \rho v'$ is identically divisible by $x - a$, and likewise by $x - b, x - c$ etc., as well as by their product v . Thus, setting

$$\frac{\pi - \rho v'}{v} = \sigma$$

we obtain for σ a polynomial in the indeterminates x, a, b, c etc. which, like ρ , is symmetric with respect to the indeterminates a, b, c etc. We can therefore find two polynomials r, s in the indeterminates x, l', l'', l''' etc. which, under the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc., become ρ, σ respectively. Following the analogy, let us denote the polynomial

$$\begin{aligned} & mx^{m-1} - (m-1)l'x^{m-2} + (m-2)l''x^{m-3} \\ & - (m-3)l'''x^{m-4} + \text{etc.} \end{aligned}$$

that is, the derivative $\frac{dy}{dx}$, by y' , so that y' becomes v' under those same substitutions. Then $p - sy - ry'$ clearly becomes $\pi - \sigma v - \rho v'$ under the same substitutions, that is, 0, and must therefore already vanish identically in itself (Article 5). We thus have the identity

$$p = sy + ry'$$

Hence, if we suppose that substituting $l' = L', l'' = L'', l''' = L'''$ etc. gives $r = R, s = S$, we also have identically

$$P = SY + RY'$$

Here S, R are polynomials in x , while P is a fixed quantity or number. It follows at once that Y and Y' cannot have a common divisor unless $P = 0$. This is precisely the second theorem of Article 6.

9.

We shall complete the proof of the first theorem by showing that, when Y and Y' have no common divisor, $P = 0$ certainly cannot hold. For this purpose, first suppose that two polynomials in the indeterminate x , namely fx and φx , have been found by the rules of Article 2, such that the identity

$$fx \cdot Y + \varphi x \cdot Y' = 1$$

holds. We write it here as

$$fx \cdot v + \varphi x \cdot v' = 1 + fx \cdot (v - Y) + \varphi x \cdot \frac{d(v - Y)}{dx}$$

or, since we have

$$\begin{aligned} v' &= (x - b)(x - c)(x - d) \dots \\ &+ (x - a) \cdot \frac{d[(x - b)(x - c)(x - d) \dots]}{dx} \end{aligned}$$

in the following form:

$$\begin{aligned} &\varphi x \cdot (x - b)(x - c)(x - d) \dots \\ &+ \varphi x \cdot (x - a) \cdot \frac{d[(x - b)(x - c)(x - d) \dots]}{dx} \\ &+ fx \cdot (x - a)(x - b)(x - c)(x - d) \dots \\ &= 1 + fx \cdot (v - Y) + \varphi x \cdot \frac{d(v - Y)}{dx} \end{aligned}$$

For brevity, we shall denote

$$fx \cdot (y - Y) + \varphi x \cdot \frac{d(y - Y)}{dx}$$

which is a polynomial in the indeterminates x, l', l'', l''' etc.,

$$\text{by } F(x, l', l'', l''' \text{ etc.})$$

Thus we have identically

$$\begin{aligned} 1 + fx \cdot (v - Y) + \varphi x \cdot \frac{d(v - Y)}{dx} \\ = 1 + F(x, \lambda', \lambda'', \lambda''' \text{ etc.}) \end{aligned}$$

We shall therefore have the identities [1]

$$\begin{aligned} \varphi a \cdot (a - b)(a - c)(a - d) \dots \\ = 1 + F(a, \lambda', \lambda'', \lambda''' \text{ etc.}) \\ \varphi b \cdot (b - a)(b - c)(b - d) \dots \\ = 1 + F(b, \lambda', \lambda'', \lambda''' \text{ etc.}) \\ \varphi c \cdot (c - a)(c - b)(c - d) \dots \\ = 1 + F(c, \lambda', \lambda'', \lambda''' \text{ etc.}) \\ \text{etc.} \end{aligned}$$

Now suppose the product of all the expressions

$$\begin{aligned} 1 + F(a, l', l'', l''' \text{ etc.}) \\ 1 + F(b, l', l'', l''' \text{ etc.}) \\ 1 + F(c, l', l'', l''' \text{ etc.}) \\ \text{etc.} \end{aligned}$$

which is a polynomial in the indeterminates a, b, c etc., l', l'', l''' etc., and is symmetric with respect to a, b, c etc., to be represented by

$$\psi(\lambda', \lambda'', \lambda''' \text{ etc.}, l', l'', l''' \text{ etc.})$$

Multiplying all the equations [1] then gives the new identity [2]

$$\pi \varphi a \cdot \varphi b \cdot \varphi c \dots = \psi(\lambda', \lambda'', \lambda''' \text{ etc.}, \lambda', \lambda'', \lambda''' \text{ etc.})$$

Further, since the product $\varphi a \cdot \varphi b \cdot \varphi c \dots$ involves the indeterminates a, b, c etc. symmetrically, we can clearly find a polynomial in the indeterminates l', l'', l''' etc. which, under the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc., becomes $\varphi a \cdot \varphi b \cdot \varphi c \dots$. Let t be this polynomial. We then also have identically [3]

$$pt = \psi(l', l'', l''' \text{ etc.}, l', l'', l''')$$

since these same substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc. turn this equation into the identity [2].

Now the very definition of the function F gives the identity

$$F(x, L', L'', L''' \text{ etc.}) = 0$$

Hence we also have identically

$$\begin{aligned} 1 + F(a, L', L'', L''' \text{ etc.}) &= 1 \\ 1 + F(b, L', L'', L''' \text{ etc.}) &= 1 \\ 1 + F(c, L', L'', L''' \text{ etc.}) &= 1 \\ &\text{etc.} \end{aligned}$$

and therefore also identically

$$\psi(\lambda', \lambda'', \lambda''' \text{ etc.}, L', L'', L''' \text{ etc.}) = 1$$

and thus identically [4]

$$\psi(l', l'', l''' \text{ etc.}, L' \cdot L'', L''' \text{ etc.}) = 1$$

Combining equations [3] and [4], and substituting $l' = L', l'' = L'', l''' = L'''$ etc., we shall therefore have [5]

$$PT = 1$$

where T denotes the value of the polynomial t corresponding to those substitutions. Since this value must be a finite quantity, P certainly cannot be $= 0$.
Q. E. D.

10.

It is now clear from the preceding results that any polynomial Y in one indeterminate x whose determinant is $= 0$ can be decomposed into factors none of which has determinant 0. For, once the greatest common divisor of the polynomials Y and $\frac{dY}{dx}$ has been found, the former is resolved into two factors. If one of these factors^{*)} again has determinant 0, it will be resolved into two factors in the same way. We shall continue in this manner until Y is finally resolved into factors none of which has determinant 0.

It is also easy to see that among these factors into which Y is resolved, at least one must have the following property: among the factors of the number expressing its degree, the number two occurs no more often than among the factors of the number m expressing the degree of the polynomial Y . That is, if we set $m = k \cdot 2^\mu$, with k denoting an odd number, then among the factors of the polynomial Y there is at least one of degree $k' \cdot 2^\nu$, where k' is also odd, and either $\nu = \mu$ or $\nu < \mu$. This assertion follows at once from the fact that m is the sum of the numbers expressing the degrees of the individual factors of Y .

^{*)}In fact, only the factor which is that common divisor can have determinant 0. But a proof of this proposition would lead us into some detours here; nor is it needed here, since the other factor, even if its determinant could also vanish, could be treated in the same way and resolved into factors.

11.

Before proceeding further, we shall explain an expression whose introduction is of great use in all investigations of symmetric functions, and which will also be very convenient for us. Suppose M is a function of some of the indeterminates a, b, c etc., and let μ be the number of them entering the expression M , without regard to any other indeterminates that M may also involve. Permuting those μ indeterminates in every possible way, both among themselves and with the remaining $m - \mu$ of a, b, c etc., produces from M other expressions similar to M . In all there are

$$m(m-1)(m-2)(m-3)\dots(m-\mu+1)$$

expressions, including M itself; we shall call their collection simply the *collection of all M* . It is then clear what is meant by the sum of all M , the product of all M , etc. Thus, for example, π is called the product of all $a - b$, v the product of all $x - a$, and v' the sum of all $\frac{v}{x-a}$, etc.

If M is symmetric with respect to some of the μ indeterminates it contains, permutations of these among themselves do not change the function M . Thus every term occurs several times in the collection of all M : namely, $1.2.3\dots\nu$ times, if ν is the number of indeterminates with respect to which M is symmetric. If M is symmetric not only with respect to ν indeterminates, but also with respect to ν' others, and again with respect to ν'' others, etc., then M remains unchanged whether two of the first ν indeterminates are interchanged, or two of the second ν' , or two of the third ν'' , etc. Thus

$$1.2.3\dots\nu. \quad 1.2.3\dots\nu'. \quad 1.2.3\dots\nu'' \text{ etc.}$$

permutations always give identical terms. If we retain only one of these identical terms each time, we therefore obtain in all

$$\frac{m(m-1)(m-2)(m-3)\dots(m-\mu+1)}{1.2.3\dots\nu.1.2.3\dots\nu'.1.2.3\dots\nu'' \text{ etc.}}$$

terms, whose collection we shall call the *collection of all M with repetitions excluded*, to distinguish it from the *collection of all M with repetitions included*. Unless an explicit qualification is given, we shall always understand repetitions to be included.

It is also easy to see that the sum of all M , or the product of all M , or more generally any symmetric function of all M , is always a symmetric function of the indeterminates a, b, c etc., whether repetitions are included or excluded.

12.

With u, x denoting indeterminates, consider now the product of all $u - (a + b)x + ab$, with repetitions excluded, and denote it by ζ . Thus ζ is the product of the following $\frac{1}{2}m(m-1)$ factors:

$$\begin{aligned} &u - (a + b)x + ab \\ &u - (a + c)x + ac \\ &u - (a + d)x + ad \\ &\text{etc.} \\ &u - (b + c)x + bc \\ &u - (b + d)x + bd \\ &\text{etc.} \\ &u - (c + d)x + cd \\ &\text{etc. etc.} \end{aligned}$$

Since this function involves the indeterminates a, b, c etc. symmetrically, we can find a polynomial in the indeterminates u, x, l', l'', l''' etc., to be denoted by z , which becomes ζ when $\lambda', \lambda'', \lambda'''$ etc. are substituted for the indeterminates l', l'', l''' etc. Finally, denote by Z the function of the indeterminates u, x alone into which z passes when the indeterminates l', l'', l''' etc. are assigned the fixed values L', L'', L''' etc.

These three functions ζ, z, Z can be regarded as polynomials of degree $\frac{1}{2}m(m-1)$ in the indeterminate u with indeterminate coefficients. These coefficients are

- for ζ , functions of the indeterminates x, a, b, c etc.
- for z , functions of the indeterminates x, l', l'', l''' etc.
- for Z , functions only of the indeterminate x .

The individual coefficients of z become those of ζ under the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc., and those of Z under the substitutions $l' = L', l'' = L'', l''' = L'''$ etc. What we have just said about the coefficients also holds for the determinants of the functions ζ, z, Z . We shall now examine these more closely, with the aim of proving the following

THEOREM. *Whenever $P = 0$ does not hold, the determinant of the function Z certainly cannot be identically $= 0$.*

13.

The proof of this theorem would indeed be very easy if we were allowed to suppose that Y could be resolved into linear factors

$$(x - A)(x - B)(x - C)(x - D) \dots$$

For it would then also be certain that Z is the product of all $u - (A+B)x + AB$, and that the determinant of the function Z is the product of the differences between pairs of the quantities

$$\begin{aligned} &(A + B)x - AB \\ &(A + C)x - AC \\ &(A + D)x - AD \\ &\text{etc.} \\ &(B + C)x - BC \\ &(B + D)x - BD \\ &\text{etc.} \\ &(C + D)x - CD \\ &\text{etc. etc} \end{aligned}$$

But this product cannot vanish identically unless one of its factors itself becomes identically $= 0$. This would imply that two of the quantities A, B, C etc. are equal, and thus that the determinant P of the polynomial Y becomes $= 0$, contrary to the hypothesis.

Setting aside this argument, which clearly starts by begging the question just as in Article 6, we now proceed directly to give a sound proof of the theorem of Article 12.

14.

The determinant of the function ζ will be the product of all the differences between pairs of $(a + b)x - ab$. The number of these differences is

$$\frac{1}{2}m(m-1)\left(\frac{1}{2}m(m-1)-1\right) = \frac{1}{4}(m+1)m(m-1)(m-2)$$

This number therefore gives the degree of the determinant of the function ζ with respect to the indeterminate x . The determinant of the function z will have the same degree. The determinant of the function Z , however, may have a lower degree, whenever some coefficients, starting from the highest power of x , vanish. Our task is now to prove that *all* the coefficients in the determinant of the function Z certainly cannot vanish.

On examining more closely the differences whose product is the determinant of the function ζ , we find that some of them—the differences between pairs of $(a + b)x - ab$ having an element in common—give

$$\text{the product of all } (a - b)(x - c)$$

while the remaining ones—the differences between pairs of $(a+b)x - ab$ whose elements are distinct—give

the product of all $(a+b-c-d)x - ab + cd$, with repetitions excluded.

The first product clearly contains each factor $a-b$ exactly $m-2$ times, and each factor $x-c$ exactly $(m-1)(m-2)$ times. We therefore readily conclude that this product is

$$= \pi^{m-2} \nu^{(m-1)(m-2)}$$

If we denote the second product by ρ , the determinant of the function ζ is thus

$$= \pi^{m-2} \nu^{(m-1)(m-2)} \rho$$

Further, let r denote the function of the indeterminates x, l', l'', l''' etc. which becomes ρ under the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc., and let R denote the function of x alone into which r passes under the substitutions $l' = L', l'' = L'', l''' = L'''$ etc. It is then clear that the determinant of the function z is

$$= p^{m-2} y^{(m-1)(m-2)} r$$

and that the determinant of the function Z is

$$= P^{m-2} Y^{(m-1)(m-2)} R$$

Since, by hypothesis, P is not $= 0$, it now remains to prove that R certainly cannot vanish identically.

15.

For this purpose we shall introduce one more indeterminate w and consider the product of all

$$(a+b-c-d)w + (a-c)(a-d)$$

with repetitions excluded. Since it involves a, b, c etc. symmetrically, it can be represented as a polynomial in the indeterminates $w, \lambda', \lambda'', \lambda'''$ etc. We shall denote this function by $f(w, \lambda', \lambda'', \lambda'''$ etc.). The number of the factors $(a+b-c-d)w + (a-c)(a-d)$ is

$$= \frac{1}{2} m(m-1)(m-2)(m-3)$$

from which we readily conclude that

$$f(0, \lambda', \lambda'', \lambda''' \text{ etc.}) = \pi^{(m-2)(m-3)}$$

and hence also

$$f(0, l', l'', l''' \text{ etc.}) = p^{(m-2)(m-3)}$$

as well as

$$f(0, L', L'', L''' \text{ etc.}) = P^{(m-2)(m-3)}$$

In general, the polynomial $f(w, L', L'', L''' \text{ etc.})$ will have degree

$$\frac{1}{2}m(m-1)(m-2)(m-3)$$

but in special cases it may have a lower degree, if some coefficients, starting from the highest power of w , happen to vanish. It is impossible, however, for the entire function to be identically $= 0$, since the equation just found shows that at least its last term does not vanish. Suppose that the highest term of the polynomial $f(w, L', L'', L''' \text{ etc.})$ having a nonvanishing coefficient is Nw^ν . If we substitute $w = x - a$, then $f(x - a, L', L'', L''' \text{ etc.})$ is clearly a polynomial in the indeterminates x, a , or, equivalently, a polynomial in x with coefficients depending on the indeterminate a . Its highest term is nevertheless Nx^ν , and thus has a fixed coefficient, independent of a , which is not $= 0$. Likewise, $f(x - b, L', L'', L''' \text{ etc.})$, $f(x - c, L', L'', L''' \text{ etc.})$ are polynomials in the indeterminate x , each with highest term Nx^ν , while the coefficients of the following terms depend respectively on b, c etc. Hence the product of the m factors

$$\begin{aligned} &f(x - a, L', L'', L''' \text{ etc.}) \\ &f(x - b, L', L'', L''' \text{ etc.}) \\ &f(x - c, L', L'', L''' \text{ etc.}) \\ &\text{etc.} \end{aligned}$$

is a polynomial in x whose highest term is $N^m x^{m\nu}$, while the coefficients of the following terms depend on the indeterminates a, b, c etc.

Next consider the product of these m factors:

$$\begin{aligned} &f(x - a, l', l'', l''' \text{ etc.}) \\ &f(x - b, l', l'', l''' \text{ etc.}) \\ &f(x - c, l', l'', l''' \text{ etc.}) \\ &\text{etc.} \end{aligned}$$

As a function of the indeterminates x, a, b, c etc., l', l'', l''' etc., symmetric with respect to a, b, c etc., it can be represented as a function of the indeterminates $x, \lambda', \lambda'', \lambda'''$ etc., l', l'', l''' etc., which we shall denote by

$$\varphi(x, \lambda', \lambda'', \lambda''' \text{ etc.}, l', l'', l''' \text{ etc.})$$

Thus

$$\varphi(x, \lambda', \lambda'', \lambda''' \text{ etc.}, \lambda', \lambda'', \lambda''' \text{ etc.})$$

is the product of the factors

$$\begin{aligned} &f(x - a, \lambda', \lambda'', \lambda''' \text{ etc.}) \\ &f(x - b, \lambda', \lambda'', \lambda''' \text{ etc.}) \\ &f(x - c, \lambda', \lambda'', \lambda''' \text{ etc.}) \\ &\text{etc.} \end{aligned}$$

and is therefore identically divisible by ρ , since it is easy to see that every factor of ρ occurs in one of those factors. We therefore set

$$\begin{aligned} &\varphi(x, \lambda', \lambda'', \lambda''' \text{ etc.}, \lambda', \lambda'', \lambda''' \text{ etc.}) \\ &= \rho\psi(x, \lambda', \lambda'', \lambda''' \text{ etc.}) \end{aligned}$$

where the symbol ψ represents a polynomial. It follows readily that we also have identically

$$\begin{aligned} &\varphi(x, L', L'', L''' \text{ etc.}, L', L'', L''' \text{ etc.}) \\ &= R\psi(x, L', L'', L''' \text{ etc.}) \end{aligned}$$

But we have proved above that the product of the factors

$$\begin{aligned} &f(x - a, L', L'', L''' \text{ etc.}) \\ &f(x - b, L', L'', L''' \text{ etc.}) \\ &f(x - c, L', L'', L''' \text{ etc.}) \\ &\text{etc.} \end{aligned}$$

which is $= \varphi(x, \lambda', \lambda'', \lambda''' \text{ etc.}, L', L'', L''' \text{ etc.})$, has highest term $N^m x^{m\nu}$. The function $\varphi(x, L', L'', L''' \text{ etc.}, L', L'', L''' \text{ etc.})$ therefore has the same highest term, and is certainly not identically $= 0$. Hence R cannot be identically $= 0$ either, and neither can the determinant of the function Z . Q. E. D.

16.

THEOREM. Let $\varphi(u, x)^*)$ denote a product of any number of factors in which the indeterminates u, x enter only linearly, that is, factors of the form

$$\begin{aligned} &\alpha + \beta u + \gamma x \\ &\alpha' + \beta' u + \gamma' x \\ &\alpha'' + \beta'' u + \gamma'' x \\ &\text{etc.} \end{aligned}$$

and let w be another indeterminate. Then the function

$$\varphi(u + w \cdot \frac{d\varphi(u, x)}{dx}, x - w \cdot \frac{d\varphi(u, x)}{du}) = \Omega$$

is identically divisible by $\varphi(u, x)$.

Proof. Setting

$$\begin{aligned} \varphi(u, x) &= (\alpha + \beta u + \gamma x)Q \\ &= (\alpha' + \beta' u + \gamma' x)Q' \\ &= (\alpha'' + \beta'' u + \gamma'' x)Q'' \\ &\text{etc.} \end{aligned}$$

we obtain for Q, Q', Q'' etc. polynomials in the indeterminates $u, x, \alpha, \beta, \gamma, \alpha', \beta', \gamma', \alpha'', \beta'', \gamma''$ etc., and

$$\begin{aligned} \frac{d\varphi(u, x)}{dx} &= \gamma Q + (\alpha + \beta u + \gamma x) \cdot \frac{dQ}{dx} \\ &= \gamma' Q' + (\alpha' + \beta' u + \gamma' x) \cdot \frac{dQ'}{dx} \\ &= \gamma'' Q'' + (\alpha'' + \beta'' u + \gamma'' x) \cdot \frac{dQ''}{dx} \\ &\text{etc.} \end{aligned}$$

$$\begin{aligned} \frac{d\varphi(u, x)}{du} &= \beta Q + (\alpha + \beta u + \gamma x) \cdot \frac{dQ}{du} \\ &= \beta' Q' + (\alpha' + \beta' u + \gamma' x) \cdot \frac{dQ'}{du} \\ &= \beta'' Q'' + (\alpha'' + \beta'' u + \gamma'' x) \cdot \frac{dQ''}{du} \\ &\text{etc.} \end{aligned}$$

^{*)}Every reader will see, even without our pointing it out, that the symbols introduced in the preceding article are confined to that article alone, and that the present meaning of the symbols φ, w must therefore not be confused with their former meaning.

When these values are substituted in the factors whose product is Ω , namely in

$$\begin{aligned} & \alpha + \beta u + \gamma x + \beta w \cdot \frac{d\varphi(u, x)}{dx} - \gamma w \cdot \frac{d\varphi(u, x)}{du} \\ & \alpha' + \beta' u + \gamma' x + \beta' w \cdot \frac{d\varphi(u, x)}{dx} - \gamma' w \cdot \frac{d\varphi(u, x)}{du} \\ & \alpha'' + \beta'' u + \gamma'' x + \beta'' w \cdot \frac{d\varphi(u, x)}{dx} - \gamma'' w \cdot \frac{d\varphi(u, x)}{du} \\ & \text{etc., respectively} \end{aligned}$$

these take the following values:

$$\begin{aligned} & (\alpha + \beta u + \gamma x)(1 + \beta w \cdot \frac{dQ}{dx} - \gamma w \cdot \frac{dQ}{du}) \\ & (\alpha' + \beta' u + \gamma' x)(1 + \beta' w \cdot \frac{dQ'}{dx} - \gamma' w \cdot \frac{dQ'}{du}) \\ & (\alpha'' + \beta'' u + \gamma'' x)(1 + \beta'' w \cdot \frac{dQ''}{dx} - \gamma'' w \cdot \frac{dQ''}{du}) \\ & \text{etc.} \end{aligned}$$

Thus Ω is the product of $\varphi(u, x)$ and the factors

$$\begin{aligned} & 1 + \beta w \cdot \frac{dQ}{dx} - \gamma w \cdot \frac{dQ}{du} \\ & 1 + \beta' w \cdot \frac{dQ'}{dx} - \gamma' w \cdot \frac{dQ'}{du} \\ & 1 + \beta'' w \cdot \frac{dQ''}{dx} - \gamma'' w \cdot \frac{dQ''}{du} \end{aligned}$$

etc., that is, of $\varphi(u, x)$ and a polynomial in the indeterminates $u, x, w, \alpha, \beta, \gamma, \alpha', \beta', \gamma', \alpha'', \beta'', \gamma''$ etc. Q. E. D.

17.

The theorem of the preceding article clearly applies to the function ζ , which we shall now represent by

$$f(u, x, \lambda', \lambda'', \lambda''' \text{ etc.})$$

so that

$$f(u + w \cdot \frac{d\zeta}{dx}, x - w \cdot \frac{d\zeta}{du}, \lambda', \lambda'', \lambda''' \text{ etc.})$$

is identically divisible by ζ . The quotient is a polynomial in the indeterminates u, x, w, a, b, c etc., symmetric with respect to a, b, c etc.; we shall represent it by

$$\psi(u, x, w, \lambda', \lambda'', \lambda''' \text{ etc.})$$

We conclude that we also have identically

$$\begin{aligned} & f(u + w \cdot \frac{dz}{dx}, x - w \cdot \frac{dz}{du}, l', l'', l''' \text{ etc.}) \\ & = z\psi(u, x, w, l', l'', l''' \text{ etc.}) \end{aligned}$$

and likewise

$$\begin{aligned} f(u + w \cdot \frac{dZ}{dx}, x - w \cdot \frac{dZ}{du}, L', L'', L''' \text{ etc.}) \\ = Z\psi(u, x, w, L', L'', L''' \text{ etc.}) \end{aligned}$$

Thus, if we represent the function Z simply by $F(u, x)$, so that

$$f(u, x, L', L'', L''' \text{ etc.}) = F(u, x)$$

holds, we have identically

$$\begin{aligned} F(u + w \cdot \frac{dZ}{dx}, x - w \cdot \frac{dZ}{du}) \\ = Z\psi(u, x, w, L', L'', L''' \text{ etc.}) \end{aligned}$$

18.

Suppose, then, that fixed values of u, x , namely $u = U, x = X$, give

$$\frac{dZ}{dx} = X', \quad \frac{dZ}{du} = U'$$

We have identically

$$\begin{aligned} F(U + wX', X - wU') \\ = F(U, X) \cdot \psi(U, X, w, L', L'', L''' \text{ etc.}) \end{aligned}$$

Whenever U' does not vanish, we may set

$$w = \frac{X - x}{U'}$$

which gives

$$\begin{aligned} F(U + \frac{XX'}{U'} - \frac{X'x}{U'}, x) \\ = F(U, X) \cdot \psi(U, X, \frac{X-x}{U'}, L', L'', L''' \text{ etc.}) \end{aligned}$$

This can also be stated as follows:

If in the function Z we set $u = U + \frac{XX'}{U'} - \frac{X'x}{U'}$, it becomes

$$F(U, X) \cdot \psi(U, X, \frac{X-x}{U'}, L', L'', L''' \text{ etc.})$$

19.

In the case where $P = 0$ does not hold, the determinant of the function Z is a function of the indeterminate x that does not vanish in itself. The number of fixed values of x for which this determinant can take the value 0 is therefore clearly finite. Thus infinitely many fixed values of x can be specified which give this determinant a value different from 0. Let X be such a value

of x , which we may also suppose to be *real*. The determinant of the function $F(u, X)$ is then not $= 0$. By Theorem II of Article 6, the functions

$$F(u, X) \quad \text{and} \quad \frac{dF(u, X)}{du}$$

can therefore have no common divisor. Suppose further that there is a fixed value of u , namely U , either real or imaginary, that is, of the form $g + h\sqrt{-1}$, which makes $F(u, X) = 0$, so that $F(U, X) = 0$. Then $u - U$ is a factor of the polynomial $F(u, X)$, and the function $\frac{dF(u, X)}{du}$ is consequently certainly not divisible by $u - U$. Suppose this function, $\frac{dF(u, X)}{du}$, takes the value U' when $u = U$ is set. It certainly cannot be the case that $U' = 0$. Now U' is clearly the value of the partial derivative $\frac{dZ}{du}$ for $u = U, x = X$. If we also denote by X' the value of the partial derivative $\frac{dZ}{dx}$ for the same values of u, x , the preceding article shows that the function Z vanishes identically under the substitution

$$u = U + \frac{XX'}{U'} - \frac{X'x}{U'}$$

and is therefore identically divisible by the factor

$$u + \frac{X'}{U'}x - (U + \frac{XX'}{U'})$$

Hence, on setting $u = xx$, we see that $F(xx, x)$ is divisible by

$$xx + \frac{X'}{U'}x - (U + \frac{XX'}{U'})$$

and thus takes the value 0 when x is taken to be a root of the equation

$$xx + \frac{X'}{U'}x - (U + \frac{XX'}{U'}) = 0$$

that is, when we set

$$x = \frac{-X' \pm \sqrt{(4UU'U' + 4XX'U' + X'X')}}{2U'}$$

These values are known to be either real or of the form $g + h\sqrt{-1}$.

It is now easy to prove that the function Y must also vanish for these same values of x . For $f(xx, x, \lambda', \lambda'', \lambda''' \text{ etc.})$ is clearly the product of all $(x - a)(x - b)$, with repetitions excluded, and thus is $= v^{m-1}$. It follows at once that

$$\begin{aligned} f(xx, x, l', l'', l''' \text{ etc.}) &= y^{m-1} \\ f(xx, x, L', L'', L''' \text{ etc.}) &= Y^{m-1} \end{aligned}$$

or $F(xx, x) = Y^{m-1}$, whose fixed value therefore cannot vanish unless the value of Y vanishes at the same time.

20.

The preceding investigations have reduced the *solution* of the equation $Y = 0$, that is, the finding of a fixed value of x , either real or of the form $g + h\sqrt{-1}$, which satisfies it, to the solution of the equation $F(u, X) = 0$, provided that the determinant of the function Y is not $= 0$. It should be observed that, if all the coefficients in Y , that is, the numbers L', L'', L''' etc., are real quantities, all the coefficients in $F(u, X)$ are also real, provided that a real quantity is taken for X , as is allowed. The degree of the secondary equation $F(u, X) = 0$ is given by the number $\frac{1}{2}m(m-1)$. Whenever m is an even number of the form $2^\mu k$, with k denoting an undetermined odd number, the degree of the secondary equation is therefore given by a number of the form $2^{\mu-1}k$.

If the determinant of the function Y becomes $= 0$, Article 10 gives another polynomial $\mathfrak{Y}$ dividing it, whose determinant is not $= 0$ and whose degree is given by a number of the form $2^\nu k$, with either $\nu < \mu$ or $\nu = \mu$. Every solution of the equation $\mathfrak{Y} = 0$ also satisfies the equation $Y = 0$. The solution of the equation $\mathfrak{Y} = 0$ is again reduced to the solution of another equation whose degree is given by a number of the form $2^{\nu-1}k$.

We therefore conclude that, in general, the solution of any equation whose degree is an even number of the form $2^\mu k$ can be reduced to the solution of another equation whose degree is of the form $2^{\mu'} k$, with $\mu' < \mu$. Whenever this number is still even, that is, μ' is not $= 0$, the same method is applied again. We shall continue in this way until we reach an equation of odd degree. All its coefficients will be real if all the coefficients of the original equation were real. Such an equation of odd degree is known to have a solution, indeed a real root. Each of the preceding equations will therefore also have a solution, either through real roots or through roots of the form $g + h\sqrt{-1}$.

It has thus been established that any polynomial Y of the form $x^m - L'x^{m-1} + L''x^{m-2} - \text{etc.}$, where L', L'' etc. are fixed real quantities, contains a factor $x - A$, where A is a quantity either real or of the form $g + h\sqrt{-1}$. In the latter case it is easy to see that Y also takes the value 0 under the substitution $x = g - h\sqrt{-1}$, and is therefore divisible by $x - (g - h\sqrt{-1})$, hence also by the product $xx - 2gx + gg + hh$. Every polynomial Y therefore certainly contains a real factor of the first or second degree. Since the same holds again for the quotient, Y can clearly be resolved into real factors of the first or second degree. This was what the present paper set out to prove.
