Another new proof of the theorem that every integral rational algebraic function of one variable can be resolved into real factors of the first or second degree

Carl Friedrich Gauss (1815)
translated by Paul Taylor and Bernard Leak (1983)

1

Although the proof of the theorem about the resolution of polynomials[1] into factors that I published in a paper sixteen years ago seemed to leave nothing to be desired in respect of rigour or simplicity, I hope that it will not come at all unwelcome to mathematicians[2] if I return again to the same very serious question, and I try to give another, no less rigorous, proof from entirely different principles. Of course that earlier proof depended, in part at least, on geometrical considerations: this one on the other hand which I aim to expound here will rest solely upon algebraic[3] principles. I reviewed the more significant of the algebraic methods which other mathematicians had up to that time applied to proving our theorem in the paper cited, and I set out copiously by what flaws they worked, of which the most serious and indeed radical is common to all those attempts which have come to my attention; I have already shown, however, that that fault is by no means inevitable in an algebraic proof. I hope that the experts will now consider that the belief formerly held is fully secured by these new studies.

2

Certain preliminaries precede the principal discussion lest anything seem lacking, because the very treatment of these additional matters, which have been passed over by others, can throw some new light on the subject. First we shall establish a property of the highest common divisor of two polynomials of one variable. Let it be said at the outset, we are always talking only of integral functions: if the product of two such functions be taken, each is called a *divisor* of it. The *degree*[4] of a divisor is determined by the exponent of highest power of the indeterminate which it contains, no regard being had to the numerical coefficient. The other properties of common divisors of functions may be dealt with fairly quickly, because in these respects they are completely analogous to the properties of the common divisors of numbers.

Suppose we are given two functions Y, Y' of the indeterminate x, of which the former has degree greater than or equal to the latter; then we may form the equations

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

[1] functiones algebraicae integrae
[2] geometri
[3] analytici
[4] ordo

by this rule, that firstly Y is divided in the usual way by Y' then Y' by the remainder Y'' from the first division (which has lower degree than Y'), then again the first remainder Y'' by the second Y''', and so on until we come to a division without a remainder, which it's clear must necessarily eventually happen, since the degrees of the polynomials[5] Y', Y'', Y''' continually decrease. It is hardly necessary to point out that these functions and likewise the coefficients q, q', q'', *etc.* are *polynomials* in x.

Then it is clear that,

I Passing backwards from the last of these equations to the first, the polynomial $Y^{(\mu)}$ is a divisor of each of the previous ones, and thus a common divisor of the given Y, Y'.

II Passing forwards from the first equation to the last, it may be seen that any common divisor of the polynomials Y, Y' also divides[6] each of the following ones, and hence also the last, $Y^{(\mu)}$.

Hence the functions Y, Y' can have no divisor of higher degree than the last, $Y^{(\mu)}$, and every common divisor of the same degree as $Y^{(\mu)}$ will be a proportional multiple of this, whence this must itself be taken as the highest common divisor.

III If $Y^{(\mu)}$ is of degree 0, *i.e.* a number, no nontrivial polynomial[7] in x can divide Y, Y': so in this case we say these polynomials have no common factor.

IV Let us take the last of our equations; then we may eliminate $Y^{(\mu-1)}$ from the antepenultimate equation; then again we may eliminate $Y^{(\mu-2)}$ by means of the previous equation and so on: then we shall have

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

if we take the functions k, k', k'', ... formed by the following rule:

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

it will follow that

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

with the upper signs applying for μ even, the lower for odd. In that case, therefore, when Y and Y' don't have a common factor, it is possible to find in this way two polynomials Z, Z' in x such that we have

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

V The converse of this proposition also holds, namely, if the equation

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

can be satisfied thus, since Z, Z' are polynomials in x, Y, Y' definitely cannot have a common factor.

[5] functiones integrae

[6] metiri

[7] nulla functio proprie sic dicta

3

Our treatment now turns to another preliminary discussion, about the transformation of symmetric functions. Let a, b, c, … be quantities, m in number, and let us denote by λ' their sum, by λ'' the sum of their products in pairs, by λ''' the sum of their products in threes, *etc.*, so that from the expansion of the product

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

arises

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

Therefore these λ', λ'', λ''', … are symmetric functions of the indeterminates a, b, c, …, *i.e.* functions in which these indeterminates occur in the same way, or, more clearly, such that they are unchanged by any permutation of these indeterminates. More generally it is apparent that any polynomial whatever of these λ', λ'', λ''', … (whether it involves these indeterminates alone or else contains yet others independent from a, b, c, …) will be a symmetric polynomial of the indeterminates a, b, c, … .

4

The converse theorem is a little less obvious. Let ρ be a symmetric function of the indeterminates a, b, c, …, which is therefore composed of a certain number of terms of the form

$$Ma^\alpha b^\beta c^\gamma \cdots,$$

where α, β, γ, denote nonnegative integers and M is a coefficient which is either a definite number, or else at least does not depend on a, b, c, … if it happens that other indeterminates besides a, b, c, … come in to the function ρ. Before anything else we may fix a certain order for these terms, to which end firstly let us arrange the indeterminates a, b, c, … in a certain arbitrary order amongst themselves; *e.g.* so that a goes in the first place, b in the second, c in the third, *etc.* Next, from the two terms

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

let us put the first higher in the order than the second if we have

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

i.e. if amongst the differences $\alpha - \alpha'$, $\beta - \beta'$, $\gamma - \gamma'$, …, the first which does not vanish is positive. Therefore terms in the same place in the order do not differ except in respect of the coefficient M, and so may be combined into one term, and we may suppose each of the terms in the polynomial ρ to have a different place in the order.

Now we observe, that if $Ma^\alpha b^\beta c^\gamma \cdots$ is the first term in the polynomial in this order, then α is necessarily bigger, or at least not less than, β. For if $\beta > \alpha$, the term $Ma^\beta b^\alpha c^\gamma \cdots$, which the polynomial ρ, being symmetrical, also involves, would come higher in the order than $Ma^\alpha b^\beta c^\gamma \cdots$, contrary to hypothesis. In the same way β will be bigger than, or at least not less than, γ, *etc.* Then each of the differences $\alpha - \beta$, $\beta - \gamma$, $\gamma - \delta$, *etc.* will be nonnegative integers.

Secondly we may observe, that if the product be taken of any polynomials whatever of the indeterminates a, b, c, … then the first term of this must necessarily be the product of the first terms of the factors. It's equally clear that the first terms of the functions λ', λ'', λ''', … are a, ab, abc, *etc.* respectively. Hence we gather that the first term of the product

$$p \; = \; M\lambda'^{\,(\alpha-\beta)}\lambda''^{\,(\beta-\gamma)}\lambda'''^{\,(\gamma-\delta)}\ldots$$

is the one which comes from $Ma^\alpha b^\beta c^\gamma \cdots$; therefore putting $\rho - p = \rho'$, the first term of the function ρ' will certainly be of lower order than the first term of the function ρ. However, clearly p, and hence ρ', are symmetric polynomials of the same a, b, c, $\ldots$. Therefore ρ' may be split up, just as was ρ before, into $p' + \rho''$, so that p' is the product of powers of λ', λ'', λ''', $\ldots$ with coefficients either determined numbers or at least not depending on a, b, c, $\ldots$ and ρ'' is indeed a symmetric polynomial of a, b, c, $\ldots$, such that its first term has lower order than that of ρ'. Continuing in the same way, it is manifest that at last ρ is reduced to the form $p + p' + p'' + \cdots$, *i.e.* will be transformed into a polynomial in λ', λ'', λ''', $\ldots$.

5

We may even restate the theorem proved in the previous section in the following way: given a polynomial, ρ, symmetrical in the indeterminates a, b, c, $\ldots$, a polynomial in some other indeterminates ℓ', ℓ'', ℓ''', $\ldots$ may be assigned such that the substitutions $\ell' = \lambda'$, $\ell'' = \lambda''$, $\ell''' = \lambda'''$, $\ldots$ it becomes ρ. Moreover it may easily be shown that *this may be done uniquely in this way.* For suppose from two distinct functions of the indeterminates ℓ', ℓ'', ℓ''', $\ldots$, say r, r', results the same function of a, b, c, $\ldots$ after the substitutions $\ell' = \lambda'$, $\ell'' = \lambda''$, $\ell''' = \lambda'''$, $\ldots$. Then therefore $r - r'$ will be a function of ℓ', ℓ'', ℓ''', $\ldots$ which does not itself vanish, but which is annihilated identically after those substitutions. This I claim to be absurd, as we may easily see, if we consider that $r - r'$ must necessarily be composed of a certain number of parts of the form

$$M\ell'^{\alpha}\ell''^{\beta}\ell'''^{\gamma}\ldots$$

whose coefficients M don't vanish, and which are different from one another in respect of their exponents, and so the highest terms of each of the parts may be written as

$$Ma^{\alpha+\beta+\gamma+\cdots}b^{\beta+\gamma+\cdots}c^{\gamma+\cdots}\cdots$$

and so are put in different places in the order, so that no way can the term of the absolutely highest degree be annihilated.

While the rest of the computation may be greatly shortened by many complete transformations after this fashion, we shall not linger on them here, since the mere possibility of transformation already suffices for our proposition.

6

Let us consider the product of $m(m-1)$ factors:

$$\begin{array}{rl} & (a-b)(a-c)(a-d)\cdots \\ \times & (b-a)(b-c)(b-d)\cdots \\ \times & (c-a)(c-b)(c-d)\cdots \\ \times & (d-a)(d-b)(d-c)\cdots \\ \times & \textit{etc.} \end{array}$$

which we shall denote by π, and which, since it involves the indeterminates a, b, c, $\ldots$ symmetrically, we may suppose to be reduced to the form of a function in λ', λ'', λ''', $\ldots$. This function becomes p if in the places of λ', λ'', λ''', $\ldots$ are substituted respectively ℓ', ℓ'', ℓ''', $\ldots$. Having done this, we shall call p the *discriminant*[8] of the polynomial

$$y = x^m - \ell' x^{m-1} + \ell'' x^{m-2} - \ell''' x^{m-3} + \cdots$$

So *e.g.* for $m = 2$ we have,

$$p = -\ell'^2 + 4\ell''$$

[8] determinans

and then for $m = 3$ it can be seen that

$$p \ = \ -\ell'^2\ell''^2 + 4\ell'^3\ell''' + 4\ell''^3 - 18\ell'\ell''\ell''' + 27\ell'''^2.$$

The discriminant of the polynomial y is therefore a function of the coefficients $\ell', \ell'', \ell''', ...$ such that by the substitutions $\ell' = \lambda'$, $\ell'' = \lambda''$, $\ell''' = \lambda'''$, ... it becomes the product of the differences amongst the pairs of quantities $a, b, c, ...$ In the case $m = 1$, *i.e.* where we have a unique indeterminate a, when no differences at all are present, it becomes convenient to adopt the number 1 as the discriminant of the polynomial y.

To fix the notion of the discriminant, one must see the coefficients of the polynomial y as indeterminate quantities. The discriminant of the polynomial with determined coefficients

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

will be a definite number P, that is the value of the function p for $\ell' = L'$, $\ell'' = L''$, $\ell''' = L'''$, ... So in the case where we suppose that Y can be resolved into simple factors

$$Y \ = \ (x - A)(x - B)(x - C)\cdots,$$

so that Y arises from

$$\upsilon \ = \ (x - a)(x - b)(x - c)\cdots$$

by putting $a = A$, $b = B$, $c = C$, ..., then so by the same substitutions λ', λ'', λ''', ... becoming $L', L'', L''', ...$ respectively, clearly P will be equal to the product of factors

$$\begin{array}{rl} & (A - B)(A - C)(A - D)\cdots \\ \times & (B - A)(B - C)(B - D)\cdots \\ \times & (C - A)(C - B)(C - D)\cdots \\ \times & (D - A)(D - B)(D - C)\cdots \\ \times & \textit{etc.} \end{array}$$

It is clear therefore that, if $P = 0$, then amongst the quantities A, B, C, ... two at least must be found to be equal; conversely if $P \neq 0$ then A, B, C, ... must necessarily be unequal. Now we observe, if we put $\frac{\mathrm{d}Y}{\mathrm{d}x} = Y'$, or

$$Y' \ = \ mx^{m-1} - (m - 1)L'x^{m-2} + (m - 2)L''x^{m-3} - \cdots,$$

that we have

$$\begin{array}{rcl} Y' & = & (x - B)(x - C)(x - D)\cdots \\ & + & (x - A)(x - C)(x - D)\cdots \\ & + & (x - A)(x - B)(x - D)\cdots \\ & + & (x - A)(x - B)(x - C)\cdots \\ & + & \textit{etc.} \end{array}$$

If therefore two of the quantities $A, B, C, ...$ are equal, *e.g.* $A = B$, then Y' will be divisible be $x - A$, so Y and Y' have a common factor $x - A$. Conversely, if we suppose that Y and Y' have a common factor, then Y' must involve a simple factor from one of these $x - A$, $x - B$, $x - C$, ... *e.g.* the first, $x - A$, which cannot be the case unless A is equal to some one of the others, B, C, D, ...

From all of this we obtain the two theorems:

I *If the discriminant of the polynomial Y is* 0 *then Y and Y' have a certain common factor, that is, if Y and Y' have no common factor then the discriminant of the polynomial Y cannot be* 0.

II *If the discriminant of the polynomial Y is not* 0, *then Y and Y' certainly cannot have a common factor, or if Y and Y' do have a common factor then necessarily the discriminant of the polynomial Y must be* 0.

7

Of course it must be noted that the full force of this very simple demonstration depends on the supposition that the polynomials Y and Y' can be resolved into simple factors: which same supposition, where the general possibility of this resolution is under examination, would be nothing but begging the question[9].

Also, however, not all who have attempted to prove the main theorem by algebraic means have defended themselves against fallacies such as this, and we have drawn attention to the origin of this specious statement of the problem already, in that everyone has just examined the *form* of the roots of equations, whilst it's required to demonstrate their rashly-supposed *existence*. But enough has been said, in the paper cited above, about the lack of rigour and clarity involved in this method.

Therefore we shall now build the results of the previous section on a more solid foundation, which otherwise we wouldn't need, at least for our proposition. We shall start from a new, similarly rather easy, beginning.

8

Let us denote by ρ the function

$$\begin{array}{cl} & \dfrac{\pi(x-b)(x-c)(x-d)\cdots}{(a-b)^2(a-c)^2(a-d)^2\cdots} \\ + & \dfrac{\pi(x-a)(x-c)(x-d)\cdots}{(b-a)^2(b-c)^2(b-d)^2\cdots} \\ + & \dfrac{\pi(x-a)(x-b)(x-d)\cdots}{(c-a)^2(c-b)^2(c-d)^2\cdots} \\ + & \dfrac{\pi(x-a)(x-b)(x-c)\cdots}{(d-a)^2(d-b)^2(d-c)^2\cdots} \\ + & \textit{etc.}, \end{array}$$

which, since π is divisible by each of the denominators, is a polynomial in the indeterminates $x, a, b, c, \ldots$. Let us now set $\frac{\mathrm{d}v}{\mathrm{d}x} = v'$, so that we have

$$\begin{array}{rcl} v' & = & (x-b)(x-c)(x-d)\cdots \\ & + & (x-a)(x-c)(x-d)\cdots \\ & + & (x-a)(x-b)(x-d)\cdots \\ & + & (x-a)(x-b)(x-c)\cdots \\ & + & \textit{etc.} \end{array}$$

Manifestly for $x = a$ we have $\rho v' = \pi$, whence we conclude that the polynomial $\pi - \rho v'$ is precisely divisible by $x - a$, and likewise by $x - b$, $x - c$, *etc.*, and so by the product v. Therefore, putting

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

σ will be a polynomial of the indeterminates $x, a, b, c, \ldots$, and indeed, just like ρ, symmetric in the indeterminates $a, b, c, \ldots$. There will therefore be two polynomials r, s in the indeterminates $x, \ell', \ell'', \ell''', \ldots$, which, by the substitutions $\ell' = \lambda'$, $\ell'' = \lambda''$, $\ell''' = \lambda'''$, ..., become ρ, σ respectively. Therefore, following the analogy, if we denote by y' the polynomial

$$mx^{m-1} - (m-1)\ell' x^{m-2} + (m-2)\ell'' x^{m-3} - (m-3)\ell''' x^{m-4} + \cdots,$$

[9] petitio principii

i.e. the derivative[10] $\frac{\mathrm{d}y}{\mathrm{d}x}$, then y' becomes by the same substitutions υ', so that $p - sy - ry'$ by the same substitutions becomes $\pi - \sigma\upsilon - \rho\upsilon'$, *i.e.* 0, so that it must now necessarily vanish identically itself (section 5): thus we have now the identical equation

$$p \;=\; sy + ry'.$$

Hence if we take, by substituting $\ell' = L'$, $\ell'' = L''$, $\ell''' = L'''$, ..., $r = R$, $s = S$, then we have identically

$$P \;=\; SY + RY'.$$

where, since S and R are polynomials of x itself, and P is in fact a determined quantity or number, it is immediately apparent that Y, Y' can have no common factor unless $P = 0$, which is the second theorem of section 6.

9

We shall deal with the proof of the first theorem as follows, to show that, in the case where Y and Y' have no common factor, then $P \neq 0$. To this end, first, using the methods of section 2, we take two polynomials in the indeterminate x, say fx and ϕx, such that the identity

$$fx.Y + \phi x.Y' \;=\; 1$$

holds, which we may write as

$$fx.\upsilon + \phi x.\upsilon' \;=\; 1 + fx.(\upsilon - Y) + \phi x.\frac{\mathrm{d}(\upsilon - Y)}{\mathrm{d}x}$$

or, since we have

$$\begin{aligned}\upsilon' \;&=\; (x-b)(x-c)(x-d)\cdots \\ &+\;\; (x-a)\frac{\mathrm{d}[(x-b)(x-c)(x-d)\cdots]}{\mathrm{d}x},\end{aligned}$$

in the following form:

$$\begin{aligned}&\phi x.(x-b)(x-c)(x-d)\cdots \\ +\;\;&\phi x.(x-a)\frac{\mathrm{d}[(x-b)(x-c)(x-d)\cdots]}{\mathrm{d}x} \\ +\;\;&fx.(x-a)(x-b)(x-c)(x-d)\cdots \\ =\;\;&1 + fx.(\upsilon - Y) + \phi x.\frac{\mathrm{d}(\upsilon - Y)}{\mathrm{d}x}.\end{aligned}$$

For the sake of brevity let us express

$$fx.(y - Y) + \phi x.\frac{\mathrm{d}(y - Y)}{\mathrm{d}x},$$

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

$$F(x, \ell', \ell'', \ell''', ...)$$

so that we have identically

$$1 + fx.(\upsilon - Y) + \phi x.\frac{\mathrm{d}(\upsilon - Y)}{\mathrm{d}x} \;=\; 1 + F(x, \lambda', \lambda'', \lambda''', ...).$$

[10] quotiens differentialis

We shall therefore have the identities [1]

$$\begin{array}{rcl} \phi a.(a-b)(a-c)(a-d)\cdots & = & 1+F(a,\lambda',\lambda'',\lambda''',...) \\ \phi b.(b-a)(b-c)(b-d)\cdots & = & 1+F(b,\lambda',\lambda'',\lambda''',...) \\ \phi c.(c-a)(c-b)(c-d)\cdots & = & 1+F(c,\lambda',\lambda'',\lambda''',...) \\ & \cdots & \end{array}$$

Taking therefore the product of all of

$$\begin{array}{c} 1+F(a,\ell',\ell'',\ell''',...) \\ 1+F(b,\ell',\ell'',\ell''',...) \\ 1+F(c,\ell',\ell'',\ell''',...) \\ etc. \end{array}$$

which will be a polynomial in the indeterminates $a, b, c, ..., \ell', \ell'', \ell''', ...$ and indeed a symmetric function in respect of $a, b, c, ...$, to be expressed by

$$\psi(\lambda',\lambda'',\lambda''',...,\ell',\ell'',\ell''',...),$$

from the multiplication of the equations [1] will result a new identity [2]

$$\pi.\phi a.\phi b.\phi c.\cdots \;=\; \psi(\lambda',\lambda'',\lambda''',...,\lambda',\lambda'',\lambda''',...).$$

It is then apparent, since the product $\phi a.\phi b.\phi c\cdots$ involves the indeterminates $a, b, c, ...$ symmetrically, that a polynomial of the indeterminates $\ell', \ell'', \ell''', ...$ can be found which, by the substitutions $\ell' = \lambda'$, $\ell'' = \lambda''$, $\ell''' = \lambda'''$, ... becomes $\phi a.\phi b.\phi c.\cdots$. Let t be that polynomial, so that [3]

$$pt \;=\; \psi(\ell',\ell'',\ell''',...,\ell',\ell'',\ell''',...)$$

holds identically, since this equation becomes [2] by the substitutions $\ell' = \lambda'$, $\ell'' = \lambda''$, $\ell''' = \lambda'''$, ...

Now it follows from the very definition of the function F that we have identically

$$F(x,L',L'',L''',...) \;=\; 0.$$

Hence we also have identically

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

and thus identically

$$\psi(\lambda',\lambda'',\lambda''',...,L',L'',L''',...) \;=\; 1$$

and so identically [4]

$$\psi(\ell',\ell'',\ell''',...,L',L'',L''',...) \;=\; 1.$$

Therefore combining equations [3] and [4] and substituting $\ell' = L'$, $\ell'' = L''$, $\ell''' = L'''$, ... we shall have

$$PT \;=\; 1$$

if by T we denote the value of the function T resulting from these substitutions. This value being necessarily a finite quantity, P certainly cannot be 0. QED

10

From what has gone before, it is already clear that any polynomial Y of one indeterminate x whose discriminant is 0 can be decomposed into factors none of which has discriminant 0. For having found the highest common factor of the functions Y and $\frac{\mathrm{d}Y}{\mathrm{d}x}$, the former is already resolved into two factors. If one of these factors[11] should again have discriminant 0 then it may be split in the same way into factors, and we shall continue in the same fashion until at last Y shall be resolved into factors none of which has discriminant 0.

It will be clear that, amongst these factors into which Y is resolved, at least one should be found that is such that, amongst the factors of its degree, 2 occurs no more often than amongst the factors of m, the degree of the function Y: say, if we put $m = k.2^{\mu}$ where k denotes an odd number, then there may be found amongst the factors of the polynomial Y at least one of degree $k'.2^{\nu}$, such that k' is also an odd number and $\nu \leq \mu$. The truth of this assertion follows immediately, since m is the sum of the degrees of the individual factors of Y .

11

Before we proceed further, we shall explain a certain expression which it is very useful to introduce into all discussions of symmetrical functions, and which will also be very convenient for us. Let us suppose that M is a function of some of the indeterminates $a, b, c, ...$, and that there are μ in number of them which enter into the expression M, disregarding the other indeterminates which M may perhaps involve. When these μ indeterminates have been permuted in every possible way, both amongst themselves and together with the remaining $m - \mu$ of $a, b, c, ...$, there arise from M other similar expressions, so that altogether there are

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

expressions, including M itself, which we shall together more simply call the *complex of all M*. From this it is immediately clear what we mean by the sum or product of all M, *etc.* Thus *e.g.* π is called the product of all $(x-a)$, v' the sum of all $\frac{v}{x-a}$, *etc.*

If perhaps M is a symmetric function in respect of some of the μ indeterminates which it contains, then the permutations amongst those don't change it, so that in the complex of all M any term whatever will occur several times, and indeed will be found in $1 \cdot 2 \cdot 3 \cdot \cdots \cdot \nu$ places, if ν is the number of indeterminates with respect to which M is symmetric. If indeed M is symmetric in respect of not just the ν indeterminates but also ν' others, and yet ν'' others, *etc.*, then M itself is unchanged if pairs of the first ν indeterminates are interchanged amongst themselves, or pairs of the second or the third, *etc.*, so that

$$1 \cdot 2 \cdot 3 \cdot \cdots \cdot \nu \cdot 1 \cdot 2 \cdot 3 \cdot \cdots \cdot \nu' \cdot 1 \cdot 2 \cdot 3 \cdot \cdots \cdot \nu'' \cdot \cdots$$

permutations always result in the identical terms. Therefore if amongst the identical terms we always retain just one then altogether we shall have

$$\frac{m(m-1)(m-2)(m-3)\cdots(m-\mu+1)}{1 \cdot 2 \cdot 3 \cdot \cdots \cdot \nu \cdot 1 \cdot 2 \cdot 3 \cdot \cdots \cdot \nu' \cdot 1 \cdot 2 \cdot 3 \cdot \cdots \cdot \nu'' \cdot \cdots}$$

terms, which together we shall call the *complex of all M omitting repetitions*, to distinguish it from the complex of all M *including repetitions.* Whenever we do not explicitly use these words, we will understand repetitions to be included.

Additionally it will easily be seen that the sum of all M, or the product of all M, or in general any symmetric function of all M will always be a symmetric function of the indeterminates $a, b, c, ...$, whether we include or exclude repetitions.

[11] It is in fact the case that no factor, besides that which was the common factor, can have discriminant 0. But the proof of this fact would here lead us away from the point; and anyway it's not necessary here, since the other factor, even if its discriminant should vanish, can be treated in the same way, and it may be split into factors.

12

Now we shall consider the product of all $u-(a+b)x+ab$ excluding repetitions (where u, x denote indeterminates), which we shall call ζ. This will therefore be a product of $\frac{1}{2}m(m-1)$ factors:

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

Since this function involves the indeterminates $a, b, c, \ldots$ symmetrically, a polynomial of the indeterminates $u, x, \ell', \ell'', \ell''', \ldots$ can be assigned, which we shall denote by z, that transforms to ζ if in the place of the indeterminates $\ell', \ell'', \ell''', \ldots$ are substituted $\lambda', \lambda'', \lambda''', \ldots$. And then we shall denote by Z the function of just the indeterminates u, x into which z transforms if we attribute to $\ell', \ell'', \ell''', \ldots$ the definite values $L', L'', L''', \ldots$.

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

for ζ, functions of the indeterminates $x, a, b, c, \ldots$,
for z, functions of the indeterminates $x, \ell', \ell'', \ell''', \ldots$,
for Z, functions solely of the indeterminate x.

Indeed the coefficients of z transform individually into coefficients of ζ by the substitutions $\ell' = \lambda'$, $\ell'' = \lambda''$, $\ell''' = \lambda'''$, ..., and moreover into coefficients of Z by the substitutions $\ell' = L'$, $\ell'' = L''$, $\ell''' = L'''$, ... The same things which we have said about the coefficients only are also true of the discriminants of the polynomials ζ, z, Z.

We shall now look more closely at these, with the object of proving the

Theorem *If $P \neq 0$ then the discriminant of the polynomial Z cannot be identically* 0.

13

The proof of this theorem would be very easy, if we were allowed to suppose that Y could be split into simple factors

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

For then Z would also be a product of all $u-(A+B)x+AB$ and the discriminant of the polynomial Z would be the product of differences of pairs of the quantities

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

This product certainly can't vanish identically unless one of its factors is identically 0, and so two of the quantities $A, B, C, \ldots$ are equal, and so the discriminant P of the polynomial Y becomes 0, contrary to hypothesis.

But having laid aside such an argument, which clearly proceeds by begging the question in the manner of section 6, we shall now give a sound proof of the result of section 12.

14

The discriminant of the polynomial ζ will be a product of all the differences of pairs of $(a+b)x-ab$, of which there are

$$\tfrac{1}{2}m(m-1)[\tfrac{1}{2}m(m-1)-1] \;=\; \tfrac{1}{4}(m+1)m(m-1)(m-2).$$

This number is therefore the degree of the discriminant of the polynomial ζ with respect to the indeterminate x. This discriminant of the polynomial z has the same degree: on the other hand the discriminant of the polynomial Z can certainly have lower degree, should some of the coefficients of the higher powers of x vanish. We must therefore demonstrate that not *all* of the coefficients in the discriminant of the polynomial Z can vanish.

Considering those differences more closely, of which the discriminant of the polynomial ζ is the product, we shall find that some of them (that is, the differences between two $(a+b)x-ab$ which have an element in common) furnish

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

and in fact the rest (the differences between two $(a+b)x-ab$ whose elements are distinct) arise as

$$\text{the product of all } (a+b-c-d)x-ab+cd \text{ without repetition.}$$

The factor $(a-b)$ clearly occurs $(m-2)$ times in the earlier product, and the factor $(x-c)$ occurs $(m-1)(m-2)$ times, so we may easily conclude that this product is

$$\pi^{m-2}\upsilon^{(m-1)(m-2)},$$

so if we denote by ρ the latter product, the discriminant of the polynomial ζ will be

$$\pi^{m-2}\upsilon^{(m-1)(m-2)}\rho.$$

Denoting by r the polynomial in the indeterminates $x, \ell', \ell'', \ell''', ...$ which becomes ρ by the substitutions $\ell' = \lambda'$, $\ell'' = \lambda''$, $\ell''' = \lambda'''$, ... and likewise by R the polynomial in just x into which r is transformed by the substitutions $\ell' = L'$, $\ell'' = L''$, $\ell''' = L'''$, ..., it is clear that the discriminant of the function z is

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

and that of Z is

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

Therefore since by hypothesis $P \neq 0$, the problem now becomes this, to demonstrate that R cannot vanish identically.

15

To this end we shall introduce another indeterminate w and consider the product of all

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

without repetitions, which, since it involves $a, b, c, ...$ symmetrically, may be expressed as a polynomial in the indeterminates $w, \lambda', \lambda'', \lambda''', ...$ Let us denote this function by $f(w, \lambda', \lambda'', \lambda''', ...)$. The number of factors $(a+b-c-d)w+(a-c)(a-d)$ will be

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

and we may easily gather that

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

and so

$$f(0, \ell', \ell'', \ell''', ...) \; = \; p^{(m-2)(m-3)}$$

and indeed

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

Generally speaking, the polynomial $f(w, L', L'', L''', ...)$ will have degree[12]

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

but in special cases it may have lower degree if perhaps it should happen that certain coefficients from the highest power of w should vanish: however, it is impossible that the function should be identically zero, since the equation found shows that at least the last term of the polynomial cannot vanish. Let us suppose that the highest term of the polynomial $f(w, L', L'', L''', ...)$ whose coefficient does not vanish is Nw^ν. If therefore we substitute $w = x - a$ it is clear that $f(x-a, L', L'', L''', ...)$ is a polynomial of the indeterminates x, a, or, which is the same thing, a polynomial in x with coefficients dependent upon the indeterminate a such that the highest term is Nx^ν and so has a definite coefficient that does not depend on a and doesn't vanish. Consequently $f(x-b, L', L'', L''', ...)$, $f(x-c, L', L'', L''', ...)$, ... will be polynomials of the indeterminate x such that the highest term of each is Nx^ν, although the coefficients of the following terms will depend respectively on b, c, ... Hence the product of the m factors

$$\begin{gathered} f(x-a, L', L'', L''', ...) \\ f(x-b, L', L'', L''', ...) \\ f(x-c, L', L'', L''', ...) \\ \textit{etc.} \end{gathered}$$

will be a polynomial in the indeterminate x whose highest term will be $N^m x^{m_\nu}$, whilst the coefficients of the following terms depend on the indeterminates $a, b, c, ...$

Now let us next consider the product of these m factors

$$\begin{gathered} f(x-a, \ell', \ell'', \ell''', ...) \\ f(x-b, \ell', \ell'', \ell''', ...) \\ f(x-c, \ell', \ell'', \ell''', ...) \\ \textit{etc.}, \end{gathered}$$

which, since it is a polynomial in the indeterminates $x, a, b, c, ..., \ell', \ell'', \ell''', ...,$ and one which is symmetric with respect to $a, b, c, ...,$ may be expressed as a polynomial in the indeterminates $x, \lambda', \lambda'', \lambda''', ..., \ell', \ell'', \ell''', ...,$ which we denote by

$$\phi(x, \lambda', \lambda'', \lambda''', ..., \ell', \ell'', \ell''', ...).$$

Therefore

$$\phi(x, \lambda', \lambda'', \lambda''', ..., \lambda', \lambda'', \lambda''', ...)$$

will be the product of the factors

$$\begin{gathered} f(x-a, \lambda', \lambda'', \lambda''', ...) \\ f(x-b, \lambda', \lambda'', \lambda''', ...) \\ f(x-c, \lambda', \lambda'', \lambda''', ...) \\ \textit{etc.}, \end{gathered}$$

[12] ad ordinem referenda erit

and so exactly divisible by ρ, since, as may easily be seen, any factor of ρ is involved in some of those factors. Therefore we may put

$$\phi(x, \lambda', \lambda'', \lambda''', ..., \lambda', \lambda'', \lambda''', ...) \;=\; \rho.\psi(x, \lambda', \lambda'', \lambda''', ...),$$

where the letter ψ denotes a polynomial. Hence it may indeed easily be deduced that, also identically,

$$\phi(x, L', L'', L''', ..., L', L'', L''', ...) \;=\; R.\psi(x, L', L'', L''', ...).$$

But above we have shown that the product of the factors

$$\begin{array}{c} f(x-a, L', L'', L''', ...) \\ f(x-b, L', L'', L''', ...) \\ f(x-c, L', L'', L''', ...) \\ \textit{etc.} \end{array}$$

which is equal to $\phi(x, \lambda', \lambda'', \lambda''', ..., L', L'', L''', ...)$, has highest term $N^m x^{m_\nu}$; therefore the polynomial $\phi(x, L', L'', L''', ..., L', L'', L''', ...)$ has the same highest term and so cannot be identically equal to 0. Therefore also R cannot be identically equal to zero nor yet indeed can the discriminant of the polynomial Z. QED

16

Theorem *Let*[13] $\phi(u, x)$ *denote a product of any number of factors, into which the indeterminates* u, x *enter only linearly, i.e. which are of the form*

$$\begin{array}{c} \alpha + \beta u + \gamma x \\ \alpha' + \beta' u + \gamma' x \\ \alpha'' + \beta'' u + \gamma'' x \\ \textit{etc.} \end{array}$$

and let w *be another indeterminate. Then the polynomial*

$$\phi(u + w\frac{\mathrm{d}\phi(u,x)}{\mathrm{d}x}, x - w\frac{\mathrm{d}\phi(u,x)}{\mathrm{d}u}) \;=\; \Omega$$

is exactly divisible by $\phi(u, x)$.

Proof Putting

$$\begin{array}{rcl} \phi(u,x) & = & (\alpha + \beta u + \gamma x)Q \\ & = & (\alpha' + \beta' u + \gamma' x)Q' \\ & = & (\alpha'' + \beta'' u + \gamma'' x)Q'' \\ & & \textit{etc.}, \end{array}$$

Q, Q', Q'', ... will be polynomials of the indeterminates u, x, α, β, γ, α', β', γ', α'', β'', γ'', ..., and

$$\begin{array}{rcl} \dfrac{\mathrm{d}\phi}{\mathrm{d}x}(u,x) & = & \gamma Q + (\alpha + \beta u + \gamma x)\dfrac{\mathrm{d}Q}{\mathrm{d}x} \\ & = & \gamma' Q' + (\alpha' + \beta' u + \gamma' x)\dfrac{\mathrm{d}Q'}{\mathrm{d}x} \\ & = & \gamma'' Q'' + (\alpha'' + \beta'' u + \gamma'' x)\dfrac{\mathrm{d}Q''}{\mathrm{d}x} \end{array}$$

[13] Perhaps without our pointing it out one will see that the symbols introduced in the previous section were restricted to that section alone, and therefore the present significance of the letters ϕ, w should not be confused with the former.

$$\begin{aligned}
&\textit{etc.}\\
\frac{\mathrm{d}\phi}{\mathrm{d}u}(u,x) &= \beta Q + (\alpha+\beta u+\gamma x)\frac{\mathrm{d}Q}{\mathrm{d}u}\\
&= \beta' Q' + (\alpha'+\beta' u+\gamma' x)\frac{\mathrm{d}Q'}{\mathrm{d}u}\\
&= \beta'' Q'' + (\alpha''+\beta'' u+\gamma'' x)\frac{\mathrm{d}Q''}{\mathrm{d}u}\\
&\textit{etc.}
\end{aligned}$$

When these values have been substituted in the factors whose product is Ω, *i.e.* in

$$\begin{gathered}
\alpha+\beta u+\gamma x+\beta w\tfrac{\mathrm{d}\phi(u,x)}{\mathrm{d}x}-\gamma w\tfrac{\mathrm{d}\phi(u,x)}{\mathrm{d}u}\\
\alpha'+\beta' u+\gamma' x+\beta' w\tfrac{\mathrm{d}\phi(u,x)}{\mathrm{d}x}-\gamma' w\tfrac{\mathrm{d}\phi(u,x)}{\mathrm{d}u}\\
\alpha''+\beta'' u+\gamma'' x+\beta'' w\tfrac{\mathrm{d}\phi(u,x)}{\mathrm{d}x}-\gamma'' w\tfrac{\mathrm{d}\phi(u,x)}{\mathrm{d}u}\\
\textit{etc.},
\end{gathered}$$

they attain the following values

$$\begin{gathered}
(\alpha+\beta u+\gamma x)(1+\beta w\tfrac{\mathrm{d}Q}{\mathrm{d}x}-\gamma w\tfrac{\mathrm{d}Q}{\mathrm{d}u})\\
(\alpha'+\beta' u+\gamma' x)(1+\beta' w\tfrac{\mathrm{d}Q'}{\mathrm{d}x}-\gamma' w\tfrac{\mathrm{d}Q'}{\mathrm{d}u})\\
(\alpha''+\beta'' u+\gamma'' x)(1+\beta'' w\tfrac{\mathrm{d}Q''}{\mathrm{d}x}-\gamma'' w\tfrac{\mathrm{d}Q''}{\mathrm{d}u})\\
\textit{etc.}
\end{gathered}$$

because of which Ω will be the product of $\phi(u,x)$ and the factors

$$\begin{gathered}
1+\beta w\tfrac{\mathrm{d}Q}{\mathrm{d}x}-\gamma w\tfrac{\mathrm{d}Q}{\mathrm{d}u}\\
1+\beta' w\tfrac{\mathrm{d}Q'}{\mathrm{d}x}-\gamma' w\tfrac{\mathrm{d}Q'}{\mathrm{d}u}\\
1+\beta'' w\tfrac{\mathrm{d}Q''}{\mathrm{d}x}-\gamma'' w\tfrac{\mathrm{d}Q''}{\mathrm{d}u}\\
\textit{etc.},
\end{gathered}$$

i.e. of $\phi(u,x)$ and a polynomial of the indeterminates u, x, w, α, β, γ, α', β', γ', α'', β'', γ'', ... QED

17

The result of the previous section is clearly applicable to the polynomial ζ, which we may henceforward write as

$$f(u,x,\lambda',\lambda'',\lambda''',...),$$

so that

$$f(u+w\frac{\mathrm{d}\zeta}{\mathrm{d}x},x-w\frac{\mathrm{d}\zeta}{\mathrm{d}u},\lambda',\lambda'',\lambda''',...)$$

is exactly divisible by ζ: the quotient, which will be a polynomial of the indeterminates $u,x,w,a,b,c,...$ symmetric with respect to $a,b,c,...$, we may write as

$$\psi(u,x,w,\lambda',\lambda'',\lambda''',...).$$

Hence we may conclude that

$$f(u+w\frac{\mathrm{d}z}{\mathrm{d}x},x-w\frac{\mathrm{d}z}{\mathrm{d}u},\ell',\ell'',\ell''',...) \;=\; z\psi(u,x,w,\ell',\ell'',\ell''',...)$$

identically, and also

$$f(u+w\frac{\mathrm{d}Z}{\mathrm{d}x},x-w\frac{\mathrm{d}Z}{\mathrm{d}u},L',L'',L''',...) \;=\; Z\psi(u,x,w,L',L'',L''',...).$$

So then we may simply write the polynomial Z as $F(u,x)$, so that

$$f(u,x,L',L'',L''',...) \;=\; F(u,x).$$

We shall have identically

$$F(u+w\frac{\mathrm{d}Z}{\mathrm{d}x}, x-w\frac{\mathrm{d}Z}{\mathrm{d}u}) \;=\; Z\psi(u,x,w,L',L'',L''',...).$$

18

If we therefore give definite values to u, x, say $u=U$, $x=X$, so that

$$\frac{\mathrm{d}Z}{\mathrm{d}x} \;=\; X', \quad \frac{\mathrm{d}Z}{\mathrm{d}u} \;=\; U',$$

then we shall have identically

$$F(U+wX', X-wU') \;=\; F(U,X)\psi(U,X,w,L',L'',L''',...).$$

Then as long as U' doesn't vanish, we may set

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

to get

$$F(U+\frac{XX'}{U'}-\frac{X'x}{U'},x) \;=\; F(U,X).\psi(U,X,\frac{X-x}{U'},L',L'',L''',...),$$

which may be stated thus:

If in the polynomial Z is substituted $u=U+\frac{XX'}{U'}-\frac{X'x}{U'}$ it becomes

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

19

When in the case, where $P\neq 0$, that the discriminant of the polynomial Z is a function of the indeterminate x that does not itself vanish, clearly the number of definite values of the indeterminate x for which the discriminant can attain the value 0 will be finite, so that infinitely many definite values can be assigned that give the discriminant a value different from 0. Let X be such a value of x (which, moreover, we may suppose to be *real*). Then the discriminant of the polynomial $F(u,X)$ will be nonzero, whence it follows by theorem II of section 6 that the polynomials

$$F(u,X) \quad \text{and} \quad \tfrac{\mathrm{d}F(u,X)}{\mathrm{d}x}$$

can't have a common factor. Now let us suppose that there exists some definite value of u, say U (which may either be real or complex[14], *i.e.* expressible in the form $g+h\sqrt{-1}$) which satisfies $F(u,X)=0$, *i.e.* such that $F(U,X)=0$. $(u-U)$ will therefore be a factor of the polynomial $F(u,X)$, and so $\frac{\mathrm{d}F(u,X)}{\mathrm{d}x}$ will therefore definitely not be divisible by $u-U$.

Therefore supposing that the latter function attains the value U', if we put $u=U$, certainly $U'\neq 0$. However it is clear that U' will be the value of the partial derivative $\frac{\mathrm{d}Z}{\mathrm{d}u}$ for $u=U$, $x=X$: if therefore we also denote by X' the value of the partial differential quotient $\frac{\mathrm{d}Z}{\mathrm{d}x}$ for the same values of u, x, it is apparent by what was shown in the previous section that the polynomial Z will vanish identically as a result of the substitution

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

[14] imaginarius

and so will be exactly divisible by the factor

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

Therefore putting $u = xx$ it is clear that $F(xx, x)$ is divisible by

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

and so will attain the value 0 if for x is put a root of the equation

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

i.e. if we substitute

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

which gives values which are either real or expressible in the form $g + h\sqrt{-1}$.

Now it may be easily shown that for the same values of x the polynomial Y must also vanish. For clearly $f(xx, x, \lambda', \lambda'', \lambda''', ...)$ is the product of all $(x - a)(x - b)$ excluding repetitions, and so equal to υ^{m-1}. Hence it immediately follows that

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

or rather $F(xx, x) = Y^{m-1}$, the definite value of which can therefore not vanish, unless at the same time the value of Y itself vanishes.

20

With the help of the preceding discussion, the *solution* of the equation $Y = 0$, *i.e.* the discovery of a definite value of x, either real or expressed in the form $g + h\sqrt{-1}$, which satisfies it, is reduced to the solution of the equation $F(u, X) = 0$, so long as the discriminant of the polynomial Y is nonzero. It's appropriate to observe that if all the coefficients in Y, *i.e.* the numbers $L', L'', L''', ...$, are real quantities then so too are all the coefficients in $F(u, X)$, since it is possible to give for X a real quantity. The degree of the secondary equation $F(u, X)$ is $\frac{1}{2}m(m - 1)$: therefore whenever m is a number of the form $2^{\mu}k$ where k is odd, then the order of the secondary equation is of the form $2^{\mu-1}k'$.

In the case when the discriminant of the polynomial Y is 0, by section 10 it may be assigned another polynomial $\mathfrak{Y}$ dividing it, whose discriminant is nonzero and whose degree is of the form $2^{\nu}k'$ such that $\nu \leq \mu$. Any solution whatever of the equation $\mathfrak{Y} = 0$ also satisfies the equation $Y = 0$: the solution of the equation $\mathfrak{Y} = 0$ may again be reduced to the solution of another equation, whose degree is of the form $2^{\nu-1}k''$

From these things we may therefore gather 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 $2^{\mu'}k'$, such that $\mu' < \mu$. So long as the number is still even, *i.e.* $\mu' \neq 0$, the same method may be applied once more, and we shall continue thus until we arrive at an equation whose degree is odd; and the coefficients of this equation will be real, so long as all the coefficients of the original equation were real. But indeed such an equation of odd degree certainly yields a solution, and indeed a real root, and so each of the preceding equations will also be soluble, either by a real root or by a root of the form $g + h\sqrt{-1}$.

Therefore it has been established, that any polynomial Y whatever of the form $x^m - L'x^{m-1} + L''x^{m-2} - \cdots$ where $L', L'', L''', ...$ are definite real quantities, involves a factor $x - A$, where A is a real quantity or one expressible in the form $g + h\sqrt{-1}$. In the latter case it may easily be seen that

Y also attains the value 0 by the substitution $x = g - h\sqrt{-1}$, and so is divisible by $x - (g - h\sqrt{-1})$ and so also by the product $xx - 2gh + gg + hh$. Therefore any polynomial whatever will indeed involve a factor of the first or second degree, and since the same applies again to the quotient, it is clear that Y can be resolved into real factors of the first or second degree. To demonstrate this was the purpose of the paper.

The Latin original of this paper appears in Volume 3, pages 33–56, of Gauss's collected works. This English translation was made by Paul Taylor in December 1983 and corrected by Bernard Leak. A summary of the proof, together with a note by Martin Hyland on its logical significance, appeared in *Eureka* **45** (1985). The LaTeX version was produced in August 2003. Thanks to Mark Wainwright for finding my notes in an old box of papers in Cambridge and returning them to me. Thanks also to Nikita Danilov for correcting several typos.

TO DO:
Indicate Gauss's footnotes with * and † instead of numbers.
Centermath with displaystyle.
Big square root in §19 with parentheses not vinculum.
Bernard's comments:
functio integra = *polynomial* throughout. So do we retain *functio* as *function* to indicate Gauss's usage, given that he doesn't always *say* "integra"? This is of interest because of the way in which polynomials are still seen as *operations*, not just as objects in themselves.
§1. "Be now a received opinion amongst the learned that..."

- "penes" is a preposition governing "peritos"
- "iudicium" is vocative singular, not genitive plural
- "esto" is second person singular imperative, so it must be addressed to "indicium"
- "an" doesn't mean "whether", except with "utrum" and similar.

"tum" is not comparative.
"factor indefinitus" means "factor" — the "indefinitus" means merely thay division of polynomials is implied, not of their values as numbers.