59.

ON MR CAYLEY'S IMPROMPTU DEMONSTRATION OF THE RULE FOR DETERMINING AT SIGHT THE DEGREE OF ANY SYMMETRICAL FUNCTION OF THE ROOTS OF AN EQUATION EXPRESSED IN TERMS OF THE COEFFICIENTS.

[*Philosophical Magazine*, v. (1853), pp. 199—202.]

FOR a considerable time past, among the few cultivators of the higher algebra, a proposition relative to the theory of the symmetrical functions of the roots of an equation has been in private circulation, which, to say nothing of the important applications of which it has been found susceptible to the calculus of forms, merits (by reason of its extreme simplicity), although, strange to say, it has, I believe, not yet obtained, a place in elementary treatises on algebra. The proposition alluded to I have reason to think first came to be observed in connexion with my well-known formulæ for Sturm's auxiliary functions in terms of the roots given in this *Magazine*. The theorem is briefly as follows. If a, b, c, &c. be the roots of an equation

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \&c. = 0,$$

any symmetric function such as $\Sigma a^\alpha b^\beta c^\gamma \ldots$, where α, β, $\gamma \ldots$ are positive integers arranged according to the order of their magnitudes in a descending (or, to speak more strictly, non-ascending) order, when expressed as a function of the coefficients, will be made up of terms of the form $p_1^{\theta_1} p_2^{\theta_2} p_3^{\theta_3} \ldots p_k^{\theta_k}$, such that $\theta_1 + \theta_2 + \theta_3 + \ldots + \theta_k$ will be equal to α for some terms, but will for no term exceed α; α being, as above described, that one of the indices α, β, $\gamma \ldots$ which is not less than any of the others.

I had prepared, and indeed despatched, a somewhat elaborate proof of this theorem for the *Cambridge and Dublin Mathematical Journal*; but on proceeding to explain my method to Mr Cayley, elicited from that sagacious analyst the following excellent impromptu, which I think too valuable to be lost; and as it is now a twelvemonth or two since our conversation on the subject took place, and the author has not cared to put it on record, I feel

myself under an obligation so to do, the more so as it entirely supersedes the comparatively inelegant demonstration of my own which I had previously intended to publish.

The method rests essentially on the following well-known theorem given by Euler relative to the partition of numbers; to wit, that the number of ways of breaking up a number n into parts is the same, whether we impose the condition that the number of parts in any partitionment shall not exceed m, or that the magnitude of any one of the parts shall not exceed m. Of this rule more hereafter—for the present to its application to the matter in hand.

Since $a, b, c \ldots$ are the roots of $x^n + p_1 x^{n-1} + \ldots$, we have

$$p_1 = a + b + c + \ldots$$

$$p_2 = ab + ac + bc + \ldots$$

$$p_3 = abc + abd + acd + \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Let $\alpha + \beta + \gamma + \ldots = n$, none of the quantities $\alpha, \beta, \gamma \ldots$ being greater than m, but $\alpha, \beta, \gamma \ldots$ being otherwise arbitrary and capable of becoming equal to any extent *inter se*. Also let $\lambda + \mu + \nu + \ldots = n$, the number of quantities λ, μ, ν, &c. being never greater than m, but the quantities themselves being otherwise arbitrary, and being capable of becoming equal to any extent *inter se*. By Euler's rule the number of systems $\alpha, \beta, \gamma \ldots$ is the same as of the systems $\lambda, \mu, \nu \ldots$, say P for each. For any system $\lambda, \mu, \nu \ldots$, we shall have $p_\lambda p_\mu p_\nu \ldots$, by virtue of the equations above written, expressible as the sum of terms of the form $\Sigma a^\alpha b^\beta c^\gamma \ldots$; it may easily be made ostensible, that *all* the combinations of $\alpha, \beta, \gamma \ldots$ subject to the above prescribed conditions must come into evidence by giving $\lambda, \mu, \nu \ldots$ all the variations of which they admit; but this is also immediately obvious indirectly from the consideration, that were it otherwise, linear relations would subsist between the different values of $p_\lambda p_\mu p_\nu \ldots$, which is obviously absurd. Hence, then, we shall be able to express the P quantities of the form $p_\lambda p_\mu \ldots$ by means of linear functions of the P quantities $\Sigma a^\alpha b^\beta c^\gamma \ldots$; and conversely, by solving the linear equations thus arising, the P quantities $\Sigma a^\alpha b^\beta c^\gamma \ldots$ may be expressed in terms of the quantities $p_\lambda p_\mu \ldots$; consequently $\Sigma a^m b^\beta c^\gamma \ldots$, where m is greater or not less than any of the quantities $\beta, \gamma \ldots$, will be expressible by means of combinations $p_\lambda p_\mu \ldots$, where the number of coefficients $p_\lambda p_\mu \ldots$ (any number of which may become identical) is for some of the combinations as great as, but for none of the combinations greater than m, as was to be proved. It will of course be seen that, for the purposes of the demonstration above given, it would have been sufficient

to have been able to assume that the number of partitions, when the greatest part is not allowed to exceed m, is not *greater* than the number of partitions when the number of parts in any one partitionment does not exceed m. The equality of these two numbers would then evince itself in the course of the demonstration as a consequence of this assumption.

A word now as to Euler's beautiful law upon which the above demonstration is based.

A corollary from it, obtained by subtracting the equation which it gives when the limiting number is taken $(m-1)$ from the equation which it gives when the limiting number is m, will be the following proposition. The number of modes of partitioning n into m parts is equal to the number of modes of partitioning n into parts, one of which is always m, and the others m or less than m. This proposition was mentioned to me by Mr N. M. Ferrers*, whose demonstration of it (probably not different from that of Euler's for the other proposition, of which it may be viewed as a corollary) is so simple and instructive, that I am sure every logician will be delighted to meet with it here or elsewhere. It affords a most admirable example of that rather uncommon kind of reasoning whereby two abstract integers are proved to be equal indirectly, by showing that neither can be greater than the other.

If there be a group of A's and a group of B's, and every A can be shown to produce a B, and every B can be shown to produce an A, no matter whether the A producing a B is the same as, or different from, the A produced by that B, it is obvious that the number of A's cannot exceed that of the B's, nor of the B's that of the A's, and the two numbers will *therefore* be equal.

Take any such grouping as 3, 3, 2, 1, say A. This may be written as

1, 1, 1
1, 1, 1
1, 1,
1,

and by reading off the columns as lines, may be transformed into the group

1, 1, 1, 1
1, 1, 1
1, 1

that is 4, 3, 2, say B.

* I learn from Mr Ferrers that this theorem was brought under his cognizance through a Cambridge examination paper set by Mr Adams of Neptune notability.

In A the number of parts is 4. In B the greatest part is 4; the others might be (although they happen not in this particular instance to be) 4, but cannot be greater than 4. And so every A in which the number of parts is 4 will give rise to a B in which 4 is one of the parts, and every other part is 4 or less, and evidently (although, as above remarked, this is immaterial to the demonstration) every such B gives reciprocally the same A from which it is itself derived; hence the number of A's and B's is equal. This is the theorem which, for the sake of distinction, I have called the Corollary to Euler's. Euler's own is proved by the same diagram; for if we define A as a grouping where the number of parts *does not exceed* 4, we get a definition of B as a grouping where the greatest part does not exceed 4, and so in general. We see that this theorem may be varied also by affirming that the number of ways in which n may be broken up, so that there shall never be less than m parts, is the same as the number of ways in which it may be broken up into parts, the greatest of which in any one way is not less than m. So, again, a similar diagram makes it apparent, that if we break up each of i numbers into parts so that the sum of the greatest parts shall not exceed (or be less than) m, the number of ways in which this can be done will be the same as the number of ways in which these i numbers can be simultaneously partitioned so that the total number of parts in any simultaneous partitionment shall never exceed (or never be less than) m; and doubtless an extensive range of analogous general theorems relative to the partitioning of numbers may be struck out by aid of the same diagram, by no means easily demonstrable unless this simple mode of conversion happen to be thought of, but in that event becoming intuitively apparent. This mode of conversion is precisely that (only applied to a more general state of things) whereby, in elementary arithmetic, it is established that m times n is the same as n times m. A consideration of the process by which the mind satisfies itself of the universality of this law, has been always sufficient to convince me of the absurdity of ascribing to an inductive process the capacity of the human mind for forming general ideas concerning necessary relations.

60.

A PROOF THAT ALL THE INVARIANTS* TO A CUBIC TERNARY FORM ARE RATIONAL FUNCTIONS OF ARONHOLD'S INVARIANTS AND OF A COGNATE THEOREM FOR BIQUADRATIC BINARY FORMS.

[*Philosophical Magazine*, v. (1853), pp. 299—303, 367—372.]

ALTHOUGH contrary to the order of exposition indicated in the title to this paper, I shall, as the simpler case, begin with establishing the theorem for a biquadratic form, say F in x, y. Let

$$F = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4,$$

$$s = ae - 4bd + 3c^2,$$

$$t = ace - ad^2 - c^3 - b^2e + 2bcd,$$

s and t are the two well-known invariants of F. I propose to prove that there can exist no other invariants to F except such as are explicit rational functions of s and t.

Let F, by means of the substitution of $fx + gy$ for x, and $f'x + g'y$ for y, be made to take the form $f_1 = x^4 + y^4 + 6mx^2y^2$. Then by the characteristic property of invariants, if $I\,(a, b, c, d, e)$ be any invariant to F of the degree q, we must have

$$I\,(1, 0, m, 0, 1) = (fg' - f'g)^{2q}\, I\,(a, b, c, d, e);$$

and it will be sufficient to prove that $I\,(1, 0, m, 0, 1)$, or say more simply $I\,(m)$, can only have the two radically distinct forms corresponding to s and t, that is

$$(s) = 1 - 3m^2 \text{ and } (t) = m - m^3,$$

any other admissible form of I being a rational explicit function of these two.

* A *Constant* in analysis is any quantity which in its own nature, or by the explicit conditions to which it is subjected, is incapable of change. An *Invariant* is an expression apparently liable to change, but which, owing to certain compensations in the modifying tendencies impressed upon it, remains as a whole unaltered. The former may be compared to a fixed point or system in mechanics; the latter to a point or system free to move, but kept at rest under the combined operation of contending forces.

It may be shown* that the parameter m in f_1 will have six different values and no more. In the first place, if we write ιx for x in f_1 (ι meaning $\sqrt{-1}$), it is obvious that m becomes $-m$. Again, let $x+\iota y$ and $x-\iota y$ be substituted in place of x and y respectively; then calling (f) the value assumed by f_1, when this substitution is made,

$$\begin{aligned}(f) &= (x+\iota y)^4 + (x-\iota y)^4 + 6m(x^2+y^2)^2 \\ &= (2+6m)(x^4+y^4) + (-12+12m)x^2y^2 \\ &= (2+6m)\left\{x^4+y^4+6\,\frac{-1+m}{1+3m}x^2y^2\right\}.\end{aligned}$$

Hence if we write

$$\frac{1}{(2+6m)^{\frac{1}{4}}}x + \frac{\iota}{(2+6m)^{\frac{1}{4}}}y \text{ for } x,$$

and

$$\frac{1}{(2+6m)^{\frac{1}{4}}}x - \frac{\iota}{(2+6m)^{\frac{1}{4}}}y \text{ for } y,$$

and call what f_1 becomes after these substitutions f_2,

$$f_2 = x^4+y^4+6\gamma(m)x^2y^2,$$

$\gamma(m)$ denoting $\dfrac{-1+m}{1+3m}$.

In like manner, by writing in f_2

$$\frac{1}{\{2+6\gamma(m)\}^{\frac{1}{4}}}x + \frac{\iota}{\{2+6\gamma(m)\}^{\frac{1}{4}}}y \text{ for } x,$$

and

$$\frac{1}{\{2+6\gamma(m)\}^{\frac{1}{4}}}x - \frac{\iota}{\{2+6\gamma(m)\}^{\frac{1}{4}}}y \text{ for } y,$$

we obtain

$$f_3 = x^4+y^4+6\gamma^2(m)x^2y^2,$$

where

$$\gamma^2(m) = \frac{-1+\dfrac{-1+m}{1+3m}}{1+3\dfrac{-1+m}{1+3m}} = \frac{-2-2m}{-2+6m} = \frac{-1-m}{-1+3m};$$

$\gamma(m)$ is a periodic function of m of the third order, for we find

$$\gamma^3(m) = \gamma^2\{\gamma(m)\} = \frac{-(1+3m)-(-1+m)}{-(1+3m)+3(-1+m)} = m.$$

It will of course be observed, also, that

$$\gamma^2(m) = -\gamma(-m) \quad \text{and} \quad \gamma(m) = -\gamma^2(-m).$$

* See Addendum [p. 607 below].

Hence

$$(-\gamma)(-\gamma)(m) = -\gamma^3(-m) = m, \quad (-\gamma^2)(-\gamma^2)(m) = -\gamma^3(-m) = m.$$

So that, in fact, the six values of the parameter are

$$\begin{array}{lll} m, & \gamma(m), & \gamma^2(m), \\ -m, & -\gamma(m), & -\gamma^2(m), \end{array}$$

forming two cycles, having the remarkable property that the terms in the same cycle are periodic functions of the third order of one another, and each term in one cycle is a periodic function of the second order of every term in the other cycle.

The modulus of substitution for passing from f_1 to f_2, that is the square of the determinant

$$\begin{bmatrix} \dfrac{1}{(2+6m)^{\frac{1}{2}}}, & \dfrac{\iota}{(2+6m)^{\frac{1}{2}}} \\ \dfrac{1}{(2+6m)^{\frac{1}{2}}}, & \dfrac{-\iota}{(2+6m)^{\frac{1}{2}}} \end{bmatrix},$$

is

$$\frac{(-2\iota)^2}{2+6m}, \text{ or } \frac{-2}{1+3m}.$$

So that if $I(m)$ be the value of any invariant of the degree q, corresponding to the form f_1, and consequently $I\left(\dfrac{m-1}{1+3m}\right)$ the same for f_2, we must have

$$I(m) = \left(\frac{1+3m}{-2}\right)^q I\left(\frac{m-1}{1+3m}\right).$$

In like manner, by means of f_3 it may be shown that we must have the further equation

$$I(m) = \left(\frac{1-3m}{-2}\right)^q I\left(\frac{m+1}{1-3m}\right).$$

These equations are easily verified for the values of (s) and (t).

Thus

$$(s) = 1 + 3m^2 = \frac{(1+3m)^2}{4}\left\{1 + 3\left(\frac{m-1}{3m+1}\right)^2\right\}$$

$$= \frac{(1-3m)^2}{4}\left\{1 + 3\left(\frac{m+1}{1-3m}\right)^2\right\},$$

$$(t) = m - m^3 = -\frac{(1+3m)^3}{8}\left\{\frac{m-1}{3m+1} - \left(\frac{m-1}{3m+1}\right)^3\right\}$$

$$= -\frac{(1-3m)^3}{8}\left\{\frac{m+1}{1-3m} - \left(\frac{m+1}{1-3m}\right)^3\right\};$$

and it is moreover obvious, that the values of (s) and (t) might have been found *à priori* by means of these functional equations.

The essential point of inference for my present purpose from the equations above, which are of the form

$$I(m) = H \times I\left(\frac{m-1}{3m+1}\right) = K \times I\left(\frac{m+1}{1-3m}\right),$$

is this, that if $I(m)$ contain any power of m, say m^i, it must also contain $(m-1)^i$ and $(m+1)^i$; in a word, $(m^3-m)^i$, which, by the way, it may be noticed, is $(t)^i$. Now, if possible, let there be any invariant $I_q(m)$ of the qth degree in m which is not a rational function of (s) and (t). If we make $2x+3y=q$, as many integer solutions as exist of this equation (in which zero values of x and y are admissible), so many functions of the form $(s)^x(t)^y$ may be formed of the degree q in m, and all of them of course invariantive functions.

As regards the general nature of any invariantive function in m, since the change of x into $-x$ in $x^4+y^4+6mx^2y^2$ introduces no change into the invariant if q be even, but changes the sign if q be odd, it follows that $I_q(m)$ is of the form $\phi(m^2)$ when q is even, and of the form $m\phi(m^2)$ when q is odd.

Let μ be the number of solutions of the equation in integers above written. Then, by linearly combining all the different values of $(s)^x(t)^y$ with $I_q(m)$, it is obvious that we may form a new invariant, say I'_q, in which the μ first occurring powers of m will be wanting, that is in which the indices $0, 2, 4 \ldots (2\mu-2)$ will be wanting when q is even, and $1, 3, 5 \ldots (2\mu-1)$ when q is odd. Hence in the former case the new invariant will contain $m^{2\mu}$, and in the latter case $m^{2\mu+1}$; and therefore, by virtue of what has been shown already, I'_q will contain $(m^3-m)^{2\mu}$ in the one case and $(m^3-m)^{2\mu+1}$ in the other.

Firstly, let $q=6i$, or $6i+2$, or $6i+4$; then $\mu=i+1$; and therefore $(m^3-m)^{2i+2}$, which is of the degree $6i+6$ in m, is contained as a factor in I which is of the degree q only, a quantity less than $6i+6$, which is absurd.

Again, secondly, let $q=6i+1$, then $\mu=i$; and $(m^3-m)^{2\mu+1}$ is of the degree $6i+3$ in m, and is contained as a factor in I, which is of the degree $6i+1$, which is again absurd.

Finally, if $q=6i+1$, or $6i+3$, $\mu=i+1$; and the factor $(m^3-m)^{2\mu+1}$ is of the degree $6i+9$, that is, in each case, greater than q, which is absurd, and thus the theorem is completely demonstrated.

It may for a moment be objected, that we have been dealing only with a particular form $x^4+6mx^2y^2+y^4$, instead of the general form

$$ax^4+4bx^3y+6cx^2y^2+4dxy^3+ey^4;$$

but the latter is always reducible to the former by means of a definite linear substitution; and if we call the modulus of the substitution, that is the square of the determinant formed by the coefficients of substitution, M, to every general invariant I_q of the qth degree, to the latter corresponds a partial form (I_q) of invariant to the former, such that

$$I_q = \frac{1}{M^q}(I_q);$$

and consequently, since every (I) is a rational function of (s) and (t), so must every I be the same of s and t; unless, indeed, it were possible to have $I_{q'} = \frac{1}{M^{q'}}(I_q)$, q' being different from and greater than q: but if this were the case, since $I_q = \frac{1}{M^q}(I_q)$, a power of M the modulus would necessarily be an invariant; but in passing from $x^4 + y^4 + 6mx^2y^2$ to $x^4 + y^4 + 6\gamma(m)\,x^2y^2$, $1 + 3m$ becomes the modulus, which we know is not an invariant. Hence the proposition is completely established for the case of the biquadratic function $(x, y)^4$*.

Now let us proceed to Aronhold's famous S and T, the invariants to the general cubic function $(x, y, z)^3$, forms equally dear to the analyst and geometer. (*Vide* Mr Salmon's *Higher Plane Curves* passim.)

The method will be precisely the same as that applied to s and t†.

We commence with the canonical form

$$x^3 + y^3 + z^3 + 6mxyz.$$

On substituting $x + y + z$, $x + \rho y + \rho^2 z$, $x + \rho^2 y + \rho z$ for x, y, z, where ρ is the cube root of unity, the above quantity takes the form

$$(3 + 6m)\{x^3 + y^3 + z^3 + 6\beta(m)\,xyz\},$$

where

$$\beta(m) = \frac{18 - 18m}{6(3 + 6m)} = \frac{1 - m}{1 + 2m},$$

a periodic function in m of the second order only, for

$$\beta^2(m) = \frac{1 + 2m - 1 + m}{1 + 2m + 2 - 2m} = m.$$

* I have made a tacit assumption throughout the foregoing demonstration (which is, however, capable of an easy proof), namely that if any fractional function of the coefficients of any form be invariantive, the numerator and denominator must be separately invariants.

† The s is Mr Cayley's property, the t belongs to Professor Boole, having been by him imparted, in the infancy of the theory, to Mr Cayley, by whom it was first given to the world, at least in its character as an Invariant.

But if we write for x in the original form ρx, it becomes

$$x^3 + y^3 + z^3 + 6\rho mxyz\,;$$

and if for x we write $\rho^2 x$, it becomes

$$x^3 + y^3 + z^3 + 6\rho^2 mxyz.$$

Hence we can by linear substitutions obtain from $x^3 + y^3 + z^3 + 6mxyz$ the three additional forms

$$x^3 + y^3 + z^3 + 6\beta(m)\,xyz,$$
$$x^3 + y^3 + z^3 + 6\gamma(m)\,xyz,$$
$$x^3 + y^3 + z^3 + 6\delta(m)\,xyz,$$

where

$$\beta(m) = \frac{1-m}{1+2m}, \quad \gamma(m) = \rho^2 \frac{1-\rho m}{1+2\rho m} = \frac{\rho^2 - m}{1+2\rho m},$$

$$\delta(m) = \rho \frac{1-\rho^2 m}{1+2\rho^2 m} = \frac{\rho - m}{1+2\rho^2 m}.$$

In all, there will be twelve values of m forming three remarkable compound cycles,

$$\begin{array}{cccc} m, & \beta(m), & \gamma(m), & \delta(m), \\ \rho m, & \rho\beta(m), & \rho\gamma(m), & \rho\delta(m), \\ \rho^2 m, & \rho^2\beta(m), & \rho^2\gamma(m), & \rho^2\delta(m). \end{array}$$

It would be beside my present object to seek to develope fully the functional relations in which the several terms of these cycles stand to one another: the interesting relations

$$\beta^2(m) = \gamma^2(m) = \delta^2(m) = m,$$
$$\beta\gamma(m) = \gamma\beta(m) = \delta(m),$$
$$\gamma\delta(m) = \delta\gamma(m) = \beta(m),$$
$$\delta\beta(m) = \beta\delta(m) = \gamma(m),$$

have been already* stated by me in another place (*Cambridge and Dublin Mathematical Journal*, March 1851†).

The (S) of the canonical form corresponding to the S of the general form is $m - m^4$; and the (T) corresponding to the T of the general form is $1 - 20m^3 - 8m^6$. (See my Calculus of Forms‡, *Cambridge and Dublin Mathematical Journal*, February 1852.) It is my object to show that any other invariant (I) to the canonical form must be a rational function of S and T.

In the first place, I observe that every invariant to any function of an odd degree i of any odd number ρ of variables must be of even dimensions; for if the degree of the dimensions be q, and D the determinant of the

[* p. 192 above.] † *Vide* Addendum [p. 607 below]. [‡ p. 311 above.]

coefficients of substitution, the invariant to the transform becomes the original invariant affected with a factor $D^{\frac{iq}{\rho}}$, where $\frac{iq}{\rho}$ must be an even integer, since otherwise the sign of this multiplier would be equivocal and indeterminable; hence when i and ρ are both odd, q must be even. Thus, then, $I(m)$ in the case before us must be an even-degreed function of m. Moreover, since the change of x into ρx converts m into ρm, and $I_q(m)$ into $\rho^q I_q(m)$, for D becomes ρ when x, y, z become $\rho x, y, z$, $I_q(m)$ must be of the form $\phi(m^3)$, $m^2\phi(m^3)$, $m\phi(m^3)$, according as the index q is of the form $6i$, $6i+2$, $6i+4$.

By precisely the same reasoning as was applied to the preceding case of (s) and (t), we see that any invariant of m which contains m^c must also contain $(1-m)^c$, $(1-\rho m)^c$, $(1-\rho^2 m)^c$, that is must contain $(m-m^4)^c$, which in fact is $(S)^c$. If, now, we consider any invariant of the qth degree in m, $I(m)$, and suppose it to be other than a rational function of (S) and (T), and if we take μ to denote the number of the solutions of $4x+6y=q$, it will follow that we may form an invariant $I'(m)$, which, when q is of the form $12i$ or $12i+6$, will contain m, and consequently $(m-m^4)^{3\mu+2}$ as a factor; and in like manner when q is of the form $12i+2$ or $12i+8$, will contain $(m-m^4)^{3\mu+2}$ as a factor; and when q is of the form $12i+4$ or $12i+10$ will contain $(m-m^4)^{3\mu+1}$ as a factor. Now when

$$q=12i, \qquad \mu=i+1,$$
$$q=12i+6, \qquad \mu=i+1;$$

when

$$q=12i+2, \qquad \mu=i,$$
$$q=12i+8, \qquad \mu=i+1;$$

when

$$q=12i+10, \qquad \mu=i+1,$$
$$q=12i+4, \qquad \mu=i+1.$$

Hence the factors dividing I_q in these several cases will be of the respective degrees

$$12i+12, \quad 12i+12; \qquad 12i+8, \quad 12i+12; \qquad 12i+16, \quad 12i+16;$$

corresponding to q, being of the several values

$$12i, \quad 12i+6; \qquad 12i+2, \quad 12i+8; \qquad 12i+10, \quad 12i+4;$$

which is clearly impossible. This proves the theorem in question (the passage being made from the canonical to the general form, as in the former part of this investigation), to wit, that S and T form what I have elsewhere termed a fundamental scale of invariants to the cubic ternary form, entering as the exclusive ingredients into every other invariant that can be derived from such form.

A word of warning is necessary before I lay down my pen: that there can be only two algebraically *independent* invariants to $(x, y)^4$ or $(x, y, z)^3$, is an immediate consequence of the canonical form of each having but one parameter; so in general there can be at most but $(n-2)$ absolutely independent invariants of $(x, y)^n$; but the point established in the preceding investigation goes to show that there can exist no other invariants than such as are *rational* functions of s and t in the one case, and S and T in the other. I shall take some other occasion to establish a similar conclusion for the forms $(x, y)^5$ and $(x, y)^6$.

I have shown that there exist three invariants to the one of the degrees 4, 8, 12, and four to the other of the degrees 2, 4, 6, 10; and I shall demonstrate that any other invariant to either form must be a rational function of those above stated. For the cubic form $(x, y)^3$ we know that there is but one invariant, namely its discriminant. Thus, then, for $n=3$, $n=4$, $n=5$, $n=6$ the number of absolutely independent invariants is $n-2$, and the number of linearly independent invariants is no greater. But this result is by no means generally true. It may be proved by means of a great law of reciprocity* which I myself originated, but unfortunately threw aside, and which M. Hermite has since demonstrated, that there are more than five linearly independent invariants to $(x, y)^7$, and more than ten, in fact twelve at least, to $(x, y)^{12}$; that is to say, it is impossible in the latter case to find ten of which all the rest shall be rational functions, although an algebraical equation connects any 11. So, again, if we take a *system* of two cubic equations, there are only five absolutely independent invariants; but there are not less than seven linearly independent fundamental invariants,

* The theorem of reciprocity alluded to in the text is the following:—If to any function $(x, y)^n$ there exists an invariant of the order m in the coefficients, then to $(x, y)^m$ there exists an invariant of the order n in the coefficients; or more generally, which is M. Hermite's addition, if to any system of functions $(x, y)^{n_1}$, $(x, y)^{n_2}$ ... $(x, y)^{n_\iota}$ there exists an invariant of the several dimensions $m_1, m_2 \ldots m_\iota$ in the respective sets of coefficients, then conversely to a system $(x, y)^{m_1}$, $(x, y)^{m_2}$ ... $(x, y)^{m_\iota}$ there exists an invariant of the dimensions $n_1, n_2 \ldots n_\iota$ in the respective sets of coefficients.

I had previously shown in this *Magazine* [p. 279 above], that Mr Cayley's formulæ for finding the number of biquadratic invariants to any function $(x, y)^n$, given in that remarkable paper of his on linear transformations [Cayley's *Collected Papers*, Vol. I., p. 95], where first dawned upon the world the clear and full-formed idea of invariants (the most original and important infused into analysis since the discovery of fluxions), could be expressed by means of the number of solutions of the equation in integers $2x+3y=n$, the square of the quadratic invariant (which only exists for even values of n) counting for one in the fundamental biquadratic scale; this is of course a direct consequence, through the law of reciprocity, of the fundamental scale to $(x, y)^4$ consisting of a quadratic and a cubic invariant. My discovery of the fundamental scale of invariants to $(x, y)^5$ and $(x, y)^6$ now enables us, through the same law of reciprocity, to express the number of distinct Quintic and Sextic invariants to $(x, y)^n$, namely as being the number of integer solutions of $x+2y+3z=\frac{n}{4}$ in the one case, and of $x+2y+3z+5t=\frac{n}{2}$ in the other.

of which any other invariant must be a rational function. In fact, if we take for our two cubics

$$U = ax^3 + 3bx^2y + 3cxy^2 + dy^3,$$

$$V = \alpha x^3 + 3\beta x^2y + 3\gamma xy^2 + \delta y^3,$$

the five coefficients of the powers of λ in the discriminant of $U + \lambda V$, each of which is of four dimensions in the two sets of coefficients combined, are all invariants of the system; but there will be besides two more, one of which is a Combinant of six dimensions, being the resultant of U and V; the other is a Combinant of two dimensions only, namely $a\delta - 3b\gamma + 3c\beta - d\alpha$. These seven together form the fundamental constituent scale.

The two last-mentioned may be expressed algebraically (by the introduction of square roots) as functions of the other five, but of course not as rational functions of the same. My attention was more particularly called to the search of a proof of the completeness of the Aronholdian system of invariants, by an inquiry as to the possibility of rigidly demonstrating that there could exist no others not made up of these, addressed to me in the spring of last year by one of the most gifted geometers of this or any other country. A morning or two after the inquiry reached me, in a walk before breakfast by the side of the ornamental water in St James's Park (a time and place by no means, according to my experience, unfavourable to the inspirations of the analytic muse), I had the satisfaction of falling upon the rather *piquant* demonstration above given, which essentially rests upon a principle, requiring no harder exercise of faith than the concession of the impossibility of a greater being contained in or proceeding out of a less.

Addendum.

On the nature of the three Cycles of four terms each which contain the twelve values of the parameter to the canonical form of a cubic function of three variables.

The equations given in the text [p. 604 above] show that each term in any one cycle is a periodic function of the *second* order of each other term in the same cycle. Moreover, it may be shown that each term in any one cycle is a periodic function of the *third* order of every term in either of the other two cycles; a sort of relation between the cycles taken *per se*, and with one another, precisely the inverse of what obtains (as already shown) for the two cycles of three terms containing the six values of the parameter to the biquadratic function of two variables. For as regards that case, it was shown

in the first part of this paper that the terms in the same cycle are periodic functions of the third order of one another, and of the second order of each of those not in the same cycle with themselves.

If we make

$$m = A, \qquad \frac{1-m}{1+2m} = B, \qquad \frac{\rho^2 - m}{1+2\rho m} = C, \qquad \frac{\rho - m}{1+2\rho^2 m} = D,$$

$$\rho A = A', \qquad \rho B = B', \qquad \rho C = C', \qquad \rho D = D',$$

$$\rho^2 A = A'', \qquad \rho^2 B = B'', \qquad \rho^2 C = C'', \qquad \rho^2 D = D''.$$

The following table will exhibit all the ternary periods that can be formed between the terms of the several cycles :—

(1)	$AB'D''$,	(4)	$BA'C''$,	(7)	$CA'D''$,	(10)	$DA'B''$,
(2)	$AC'B''$,	(5)	$BC'D''$,	(8)	$CB'A''$,	(11)	$DB'C''$,
(3)	$AD'C''$,	(6)	$BD'A''$,	(9)	$CD'B''$,	(12)	$DC'A''$.

For instance, as an example of the meaning of the table, take line (8), namely $CB'A''$. This indicates that A'' is formed from B' and C from A'' in the same way as B' from C, and of course A'' from C in the same way as C from B' and B' from A'', &c. By means of this table it will easily be seen that a term in each of two cycles being given, the term in the third which forms with the given two a ternary period may immediately be assigned.

The remarks which I have to add on the nature of the equations for finding the parameter m, as well for $(x, y)^4$ as for $(x, y, z)^3$, will be given hereafter.