885.

ON THE DIOPHANTINE RELATION, $y^2 + y'^2 = $ SQUARE.

THE diophantine relation $y^2 + y'^2 = $ Square, where y is a function of x, and y' denotes $\dfrac{dy}{dx}$, is considered by Prof. Sylvester in his paper "On Reducible Cyclodes," *Proc. Lond. Math. Soc.*, t. I. (1865—66), pp. 137—160. It is at once seen that there exists a solution

$$y = (x + a)^\alpha (x + b)^\beta (x + c)^\gamma (x + d)^\delta \dots,$$

where the roots a, b, c, d, ... are essentially unequal, and the number of simple factors $x + a$, $x + b$, $x + c$, $x + d$, ... is even; the exponents α, β, γ, δ, ... are taken to be positive integer numbers. Sylvester assumes, and it will be shown, that the factors must separate themselves into two sets, or, as he calls them, diptychs, each containing the same number of simple factors and such that the sum of the exponents for the one diptych is equal to the sum of the exponents for the other diptych; viz. the form is $y = UU_1$, where

$$U = (x + a)^\alpha (x + b)^\beta \dots, \quad U_1 = (x + a_1)^{\alpha_1} (x + b_1)^{\beta_1} \dots,$$

with the same number of simple factors, and with the relation $\alpha + \beta + \dots = \alpha_1 + \beta_1 + \dots$ between the exponents. Hence, if the number of simple factors be called the class and the sum of the exponents be called the order, the class and the order are each of them even; or, what is the same thing, the semi-class (say μ) and the semi-order (say ν) are each of them integral.

The separation of the factors into two diptychs is a remarkable theorem. I consider the analytical theory; for greater simplicity, first in the case, class = 2, and secondly in the case, class = 4; but it is easy to see that the like process is applicable to the case of any even value whatever of the class.

I write as usual $i = \sqrt{-1}$; the equation $y^2 + y'^2$ = square, implies $y + iy'$ = square, and $y - iy'$ = square; at least this is so, save as to a common denominator, as will appear.

First, if the class is $= 2$; we have

$$y = (x + a)^\alpha (x + b)^\beta;$$

hence

$$y + iy' = y \left(1 + \frac{i\alpha}{x + a} + \frac{i\beta}{x + b} \right),$$

$$y - iy' = y \left(1 - \frac{i\alpha}{x + a} - \frac{i\beta}{x + b} \right),$$

say these are $= \dfrac{(x + l)^2 \, y}{x + a \, . \, x + b}$ and $\dfrac{(x + m)^2 \, y}{x + a \, . \, x + b}$ respectively; and, this being so, we have

$$y^2 + y'^2 = \frac{y^2 (x + l)^2 (x + m)^2}{(x + a)^2 (x + b)^2}, \; = (x + a)^{2\alpha - 2} (x + b)^{2\beta - 2} (x + l)^2 (x + m)^2.$$

It is to be shown that the assumed relations lead to $\alpha = \beta$. Resolving the last-mentioned expressions for $y + iy'$, $y - iy'$ each into simple fractions, we have

$$i\alpha (b - a) = (l - b)^2, \quad -i\alpha (b - a) = (m - b)^2,$$

$$i\beta (a - b) = (l - a)^2, \quad -i\beta (a - b) = (m - a)^2.$$

Hence

$$(l - b)^2 + (m - b)^2 = 0, \quad (l - a)^2 + (m - a)^2 = 0;$$

these cannot give

$$(l - b) + i (m - b) = 0, \quad (l - a) + i (m - a) = 0,$$

with the same sign for i in the two equations; for we should then have

$$(1 + i)(b - a) = 0,$$

but $1 + i$ is not $= 0$, and a, b are essentially unequal. Hence, taking (as we may do) $+ i$ in the first equation, we must have $- i$ in the second equation, and the two equations are

$$l - b + i (m - b) = 0, \text{ that is, } l + im = (1 + i) b,$$

$$l - a - i (m - a) = 0, \quad \text{,,} \quad l - im = (1 - i) a,$$

and thence

$$2l = (1 + i)(b - ia),$$

$$2m = (1 + i)(b + ia).$$

Hence also

$$2 (l - b) = \quad (1 - i)(a - b), \quad 2i (m - b) = (1 - i)(b - a),$$

$$2 (l - a) = -(1 + i)(a - b), \quad 2i (m - a) = (1 + i)(b - a);$$

consequently

$$2 (l - b)^2 = -i (a - b)^2, \; = -2i\alpha (a - b),$$

$$2 (l - a)^2 = \quad i (a - b)^2, \; = \quad 2i\beta (a - b).$$

Hence $\alpha = \beta = \frac{1}{2}(a-b)$, and the solution thus is

$$y = (x+a)^\alpha (x+b)^\alpha, \quad \alpha = \frac{1}{2}(a-b),$$

$$l = \frac{1}{2}\{a+b+i(a-b)\},$$

$$m = \frac{1}{2}\{a+b-i(a-b)\},$$

$$y^2 + y'^2 = (x+a)^{2\alpha-2}(x+b)^{2\alpha-2}(x+l)^2(x+m)^2.$$

The class is here $= 2$, and the order is $= 2\alpha$; considering the order as given, say it is $= 2\nu$, we have $\alpha = \nu$, and the equation $\nu = \frac{1}{2}(a-b)$ then shows that one of the roots a, b is arbitrary. Taking it to be a, we have $b = a - 2\nu$, or the solution, class 2 and order 2ν, is

$$y = (x+a)^\nu (x+a-2\nu)^\nu,$$

$$l = \alpha - \nu + i\nu, \quad m = \alpha - \nu - i\nu,$$

$$y^2 + y'^2 = (x+a)^{2\nu-2}(x+a-2\nu)^{2\nu-2}(x+l)^2(x+m)^2.$$

Considering next for the case, class $= 4$, the solution

$$y = (x+a)^\alpha (x+b)^\beta (x+c)^\gamma (x+d)^\delta,$$

we have

$$y + iy' = y\left(1 + \frac{i\alpha}{x+a} + \frac{i\beta}{x+b} + \frac{i\gamma}{x+c} + \frac{i\delta}{x+d}\right),$$

$$y - iy' = y\left(1 - \frac{i\alpha}{x+a} - \frac{i\beta}{x+b} - \frac{i\gamma}{x+c} - \frac{i\delta}{x+d}\right);$$

or, putting these

$$= \frac{(x+l)^2(x+p)^2\,y}{x+a\,.\,x+b\,.\,x+c\,.\,x+d} \quad \text{and} \quad \frac{(x+m)^2(x+q)^2\,y}{x+a\,.\,x+b\,.\,x+c\,.\,x+d}$$

respectively, we have

$$y^2 + y'^2 = \frac{y^2(x+l)^2(x+p)^2(x+m)^2(x+q)^2}{(x+a)^2(x+b)^2(x+c)^2(x+d)^2},$$

$$= (x+a)^{2\alpha-2}(x+b)^{2\beta-2}(x+c)^{2\gamma-2}(x+d)^{2\delta-2}(x+l)^2(x+p)^2(x+m)^2(x+q)^2.$$

Also, by decomposing the expressions for $y + iy'$, $y - iy'$ into simple fractions and comparing with the original values, we find

$$i\alpha\,(b-a)(c-a)(d-a) = (a-\ l)^2(a-p)^2,$$

$$i\beta\,(a-b)(c-b)(d-b) = (b-\ l)^2(b-p)^2,$$

$$i\gamma\,(a-c)(b-c)(d-c) = (c-\ l)^2(c-p)^2,$$

$$i\delta\,(a-d)(b-d)(c-d) = (d-\ l)^2(d-p)^2,$$

$$-i\alpha\,(b-a)(c-a)(d-a) = (a-m)^2(a-q)^2,$$

$$-i\beta\,(a-b)(c-b)(d-b) = (b-m)^2(b-q)^2,$$

$$-i\gamma\,(a-c)(b-c)(d-c) = (c-m)^2(c-q)^2,$$

$$-i\delta\,(a-d)(b-d)(c-d) = (d-m)^2(d-q)^2.$$

Hence

$$(a - l)^2 (a - p)^2 + (a - m)^2 (a - q)^2 = 0,$$
$$(b - l)^2 (b - p)^2 + (b - m)^2 (b - q)^2 = 0,$$
$$(c - l)^2 (c - p)^2 + (c - m)^2 (c - q)^2 = 0,$$
$$(d - l)^2 (d - p)^2 + (d - m)^2 (d - q)^2 = 0;$$

we cannot from these obtain *three* equations

$$(a - m)(a - q) - i(a - l)(a - p) = 0,$$
$$(b - m)(b - q) - i(b - l)(b - p) = 0,$$
$$(c - m)(c - q) - i(c - l)(c - p) = 0,$$

with the same sign for i; in fact these would give

$$(1 + i)(b - c)(c - a)(a - b) = 0,$$

but $1 + i$ is not $= 0$, and the a, b, c are essentially unequal. Hence we must have equations such as

$$(a - m)(a - q) - i(a - l)(a - p) = 0; \quad (c - m)(c - q) + i(c - l)(c - p) = 0,$$
$$(b - m)(b - q) - i(b - l)(b - p) = 0; \quad (d - m)(d - q) + i(d - l)(d - p) = 0,$$

two of them with $-i$, and two of them with $+i$; viz. the a, b, c, d divide themselves into pairs which are taken to be a, b and c, d.

We hence easily obtain

$$a + b - m - q - i(a + b - l - p) = 0, \quad ab - mq - i(ab - lp) = 0,$$
$$c + d - m - q - i(c + d - l - p) = 0, \quad cd - mq - i(cd - lp) = 0,$$

and thence

$$a + b - c - d = i(a + b + c + d) - 2i(l + p),$$
$$ab - cd = i(ab + cd) \qquad - 2ilp.$$

Forming from these values of $l + p$, lp the expression for $2i(a - l)(a - p)$, we find $2i(a - l)(a - p) = (i + 1)(a - c)(a - d)$; and we have thus the set of equations

$$2i(a - l)(a - p) = (i + 1)(a - c)(a - d),$$
$$2i(b - l)(b - p) = (i + 1)(b - c)(b - d),$$
$$2i(c - l)(c - p) = (i - 1)(c - a)(c - b),$$
$$2i(d - l)(d - p) = (i - 1)(d - a)(d - b).$$

Hence also

$$2(a - l)^2 (a - p)^2 = - i(a - c)^2 (a - d)^2,$$
$$2(b - l)^2 (b - p)^2 = - i(b - c)^2 (b - d)^2,$$
$$2(c - l)^2 (c - p)^2 = \quad i(c - a)^2 (c - b)^2,$$
$$2(d - l)^2 (d - p)^2 = \quad i(d - a)^2 (d - b)^2;$$

and, substituting these values in a former set of equations, we obtain

$$2\alpha(b - a) = -(a - c)(a - d),$$
$$2\beta(a - b) = -(b - c)(b - d),$$
$$2\gamma(d - c) = \quad (c - a)(c - b),$$
$$2\delta(c - d) = \quad (d - a)(d - b);$$

and thence

$$2(\alpha + \beta) = \quad a + b - c - d,$$
$$2(\gamma + \delta) = -(c + d - a - b),$$

that is, $\alpha + \beta = \gamma + \delta$; viz. there are, in this case also, two diptychs.

If, as before, the order is taken to be $= 2\nu$, then $\alpha + \beta = \nu$, $\gamma + \delta = \nu$; supposing that ν is a given positive integer, and that α, β, γ, δ are positive integers satisfying these equations $\alpha + \beta = \nu$, $\gamma + \delta = \nu$, then the last-mentioned four equations between α, β, γ, δ and a, b, c, d are equivalent to three relations serving to determine the differences of a, b, c, d (say $a - d$, $b - d$, $c - d$) in terms of α, β, γ, δ. And we then further have

$$(a-l)(a-p) = -(1-i)\,\alpha\,(b-a), \quad (a-m)(a-q) = -(1+i)\,\alpha\,(b-a),$$
$$(b-l)(b-p) = -(1-i)\,\beta\,(a-b), \quad (b-m)(b-q) = -(1+i)\,\beta\,(a-b),$$
$$(c-l)(c-p) = \quad (1+i)\,\gamma\,(d-c), \quad (c-m)(c-q) = \quad (1-i)\,\gamma\,(c-d),$$
$$(d-l)(d-p) = \quad (1+i)\,\delta\,(c-d), \quad (d-m)(d-q) = \quad (1-i)\,\delta\,(d-c),$$

each set equivalent to two equations; or, as these may be written,

$$2(l + p) = a + b + c + d + i(a + b - c - d),$$
$$2lp \quad\quad = ab + cd \quad\quad + i(ab - cd),$$
$$2(m + q) = a + b + c + d - i(a + b - c - d),$$
$$2mq \quad\quad = ab + cd \quad\quad - i(ab - cd),$$

serving to determine l, p, m, q in terms of a, b, c, d.

Observe also that, u being arbitrary, we have

$$2(u - l)(u - p) = (1 + i)(u - a)(u - b) + (1 - i)(u - c)(u - d),$$
$$2(u - m)(u - q) = (1 - i)(u - a)(u - b) + (1 + i)(u - c)(u - d),$$

(which equations, writing therein $u = a$, b, c, or d, in fact reproduce the two systems of four equations).

We have also

$$l + p + m + q = a + b + c + d, \quad l + p - m - q = i(a + b - c - d),$$
$$lp + mq \quad\quad = ab + cd, \quad\quad lp - mq \quad\quad = i(ab - cd);$$

and moreover

$$4(l - p)^2 = \quad 2i\{(a-b)^2 - (c-d)^2\} + 4(a+b)(c+d) - 8(ab + cd),$$
$$4(m - q)^2 = -2i\{(a-b)^2 - (c-d)^2\} + 4(a+b)(c+d) - 8(ab + cd),$$

which equations, combined with the foregoing values of $2(l + p)$ and $2(m + q)$, give the values of l, p, m, q. We have thus the complete solution for the case class $= 4$, order $= 20$; say

$$y = (x + a)^\alpha (x + b)^\beta \cdot (x + c)^\gamma (x + d)^\delta; \quad \alpha + \beta = \gamma + \delta = \nu,$$
$$y^2 + y'^2 = (x + a)^{2\alpha-2}(x + b)^{2\beta-2}(x + c)^{2\gamma-2}(x + d)^{2\delta-2}(x + l)^2(x + p)^2(x + m)^2(x + q)^2,$$

with the foregoing relations between the constants.