On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees.

By L. J. MORDELL, Manchester College of Technology.

[*Received* 1 May, *read* 22 May, 1922.]

§ 1. Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results*, as that of finding the rational solutions†, or say for shortness, the solutions of indeterminate equations of genus unity of the forms

$$\left.\begin{aligned} \zeta^2 &= a\xi^4 + b\xi^3\eta + c\xi^2\eta^2 + d\xi\eta^3 + e\eta^4 \\ y^2 &= ax^4 + bx^3 + cx^2 + dx + e \end{aligned}\right\} \quad \text{.........(1)},$$

$$0 = f(x, y, z) \quad \text{.......................................(2)},$$

where f is a ternary homogeneous cubic in x, y, z, including as a particular case

$$y^2 = 4x^3 - g_2 x - g_3 \quad \text{.....................(3)};$$

and there is no loss of generality in assuming that the coefficients of all equations in this paper are integers. Our present knowledge is based on three types of results, of which the first enables us in general to find an infinite number of solutions when a finite number have already been found, e.g. by trial, and has been known in principle for some centuries. For a value of x, y, z, satisfying equation (2) defines a rational point P on the cubic curve (2); and the tangent at P will meet the cubic in another rational point P_1 different in general from P. Not only can this process be repeated with P_1, but if another rational point Q is known, then the intersection of the chord PQ with the cubic gives also a rational point. This process can in general be continued indefinitely.

The analytical interpretation is obvious from equation (3). For if we know several solutions, say x_1, y_1; x_2, y_2, ..., we define arguments u_1, u_2 ... by writing

$$x_1 = \wp(u_1), \quad y_1 = \wp'(u_1), \quad \text{etc.}$$

in the usual notation of elliptic functions. The addition formula then shows that the formulae

$$x = \wp(m_1u_1 + m_2u_2 \ldots), \; y = \wp'(m_1u_1 + m_2u_2 \ldots) \quad \ldots(4)$$

[*] See, for example, vol. II. of Dickson's *History of the Theory of Numbers.*

[†] We may suppose that ξ, η, ζ in equation (1), and x, y, z in equation (2) are all integers.

give in general an infinite number of solutions by taking for m_1, m_2, ... all integer values, positive, negative and zero..

The second type of result is that certain classes of equations, e.g.

$$x^3+y^3+pz^3=0$$

where $p>2$ is a prime of the forms $9n+2$, $9n+5$ or the square of such a prime, has only the solution

$$x=1,\ y=-1,\ z=0.$$

The third result* is that all the solutions of equations (1), (2) can be found if we know only one solution, and all the solutions of equation (3), where g_2, g_3 are the well-known invariants of the quartic (1) [written with binomial coefficients a, $4b$, $6c$, $4d$, e] or multiples of the fundamental invariants of the cubic (2). Conversely we can solve completely equation (3) if we know the complete solution of equations (1) or (2).

I shall now prove that if any of these equations (1, 2, 3) have an infinite number of solutions, then the method of infinite descent applies, that is to say, all the solutions can be expressed rationally in terms of a finite number by means of the classic method. In other words, the solution of equation (3) is given by (4) where u_1, u_2 ... are *finite* in number.

§ 2. The last result mentioned and some developments therefrom will be required later, so that a very simple proof may be given here. There is no loss of generality in considering the equation (the coefficients c, d, etc. need not be integers),

$$\zeta^2=\xi^4+6c\xi^2\eta^2+4d\xi\eta^3+e\eta^4,$$

of which one solution is given by $\xi=1$, $\eta=0$, or say

$$y^2=x^4+6cx^2+4dx+e$$

with a known rational solution $x=\infty=1/0$. Put

$$2s=x^2+c+y$$

so that s is rational if both x and y are.

By eliminating y

$$4s^2-4s(x^2+c)=4cx^2+4dx+e-c^2,$$

or $$4(c+s)x^2+4dx=4s^2-4sc+c^2-e,$$

whence $2x(s+c)=-d\pm[d^2+(s+c)(4s^2-4sc+c^2-e)]^{\frac{1}{2}}$,

reducing to $$2x(s+c)=-d+t,$$

where $$t^2=4s^3-g_2s-g_3,$$

* See my paper "Indeterminate equations of the third and fourth degree." *Quarterly Journal of Pure and Applied Mathematics*, vol. XLV, 1914, pages 180, 186. Particular cases have been given by Sylvester and other writers.

and g_2, g_3 are the well-known invariants of the quartic with binomial coefficients. Clearly x and y are rational if s and t are. The transformation is birational, and by putting

$$s = \wp(u), \quad t = \wp'(u)$$

we can establish a one to one correspondence between the points on the quartic, and a period parallelogram in the u plane. Further, the parabola

$$y = -x^2 + \lambda x + \mu$$

is changed into $$2s - c = \frac{\lambda}{2}\left(\frac{t-d}{s+c}\right) + \mu,$$

or say the parabola $$t = Ns^2 + Ls + M.$$

This meets the cubic in four points corresponding to, say, u_1, u_2, u_3, u_4, for which

$$u_1 + u_2 + u_3 + u_4 \equiv 0 \qquad (\text{mod } \omega_1, \omega_2)$$

where ω_1, ω_2 are the periods of the $\wp$ function.

For the general quartic (page 180 of my *Quarterly* paper)

$$z^2 = ax^4 + 4bx^3y \dots + ey^4 \equiv f(x, y),$$

when we know one solution x_0, y_0, the general solution is given by

$$x = 2x_0 (tf_0^{\frac{3}{2}} + g_0) + \frac{\partial f_0}{\partial y_0}(h_0 - sf_0),$$

$$y = 2y_0 (tf_0^{\frac{3}{2}} + g_0) - \frac{\partial f_0}{\partial x_0}(h_0 - sf_0),$$

where $f_0 = f(x_0, y_0)$, h_0 is the Hessian $(b^2 - ac)p_0^4 + \dots$ and g_0 the sextic covariant of the quartic f_0. Also

$$t^2 = 4s^3 - g_2 s - g_3 \dots\dots\dots\dots\dots\dots\dots\dots(3).$$

§ 3. It will be convenient to prove now another result which will be required later. It has been shown in my *Quarterly* paper that all the integer solutions of the equation in g_1; h, a

$$g_1^2 = h^3 - G_2 ha^2 - G_3 a^3 \quad \dots\dots\dots\dots\dots\dots(5),$$

with a odd and prime to h, are given by taking

$$a = F(p, q) = (A, B, C, D, E)(p, q)^4,$$

$$h = H(p, q) = (B^2 - AC)p^4 + \dots \quad \dots\dots\dots\dots\dots(6),$$

$$2g_1 = G(p, q)$$

where $F(p, q)$ is a representative of the classes (finite in number) of binary quartics with invariants

$$g_2 = 4G_2, \quad g_3 = 4G_3,$$

$-H(p,q)$ is the Hessian and $G(p,q)$ the sextic covariant of $F(p,q)$. Further, p and q are any coprime integers for which a is odd and prime to h.

The new result is that these formulae (6) still give the solution if only a is prime to h, so that a may also be even—provided of course that p, q are any coprime integers for which a is prime to h. For the well-known syzygy of the quartic (writing G for shortness instead of $G(p, q,)$ etc.) gives

$$G^2 = 4H^3 - 4G_2HF^2 - 4G_3F^3,$$

showing that (6) is a solution of (5).

Conversely, if g_1, h, a are given and h is prime to a, it will be shown that we can find a quartic with invariants, $4G_2$, $4G_3$,

$$(a, b, c, d, e)(x, y)^4 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(7),$$

where a, b, etc., are integers, and b and hence $h = b^2 - ac$ are both prime to a. This quartic will be equivalent to a representative of the finite number of classes of binary quartics, whence

$$a = F(p, q), \quad h = H(p, q).$$

For suppose c, d, e are given by

$$\begin{aligned} ac &= b^2 - h, \\ a^2d &= b^3 - 3bh + 2g_1, \\ a^3e &= 4G_2a^2 - 3h^2 + b^4 - 6b^2h + 8bg_1; \end{aligned}$$

then it is easily verified [see page 171 of my *Quarterly* paper] that the invariants of the quartic (7) are $4G_2$, $4G_3$, that is

$$\begin{aligned} 4G_2 &= ae - 4bd + 3c^2, \\ 4G_3 &= ace + 2bcd - ad^2 - b^2e - c^3 \quad \ldots\ldots\ldots\ldots(7). \end{aligned}$$

It will now be shown that c, d, e are integers for a suitable value of b, namely,

$$b \equiv g_1/h \quad (\text{mod } a^2).$$

For
$$\begin{aligned} ac &\equiv (g_1^2 - h^3)/h^2 \quad (\text{mod } a) \\ &\equiv 0 \quad (\text{mod } a) \end{aligned}$$

from equation (5), so that c is an integer.

Also
$$\begin{aligned} a^2d &\equiv g_1^3/h^3 - g_1 \quad (\text{mod } a^2) \\ &\equiv g_1(g_1^2 - h^3)/h^3 \quad (\text{mod } a^2) \\ &\equiv 0 \quad (\text{mod } a^2) \end{aligned}$$

from equation (5), so that d is an integer.

Also from equation (7) ae and $(ac - b^2)e$ are integers, that is, ae and he are integers. Hence, as a is prime to h, e is also an integer. This proves the result.

§ 4. Consider now equation (1) which is taken in the form

$$x^4 - px^3y - qx^2y^2 - rxy^3 - sy^4 = az^2 \quad \text{............(8)},$$

where there is no loss of generality in supposing x is prime to y, and that a is not a perfect square. Suppose also that the quartic field $K(\theta)$ is defined by the equation

$$\theta^4 - p\theta^3 - q\theta^2 - r\theta - s = 0,$$

which is supposed to have no rational linear factors in θ. Hence θ is either a root of an irreducible quartic or of an irreducible quadratic. In the latter case the field is generated by the roots of both quadratics. The left-hand side of (8) splits up into factors

$$x - \theta y \quad \text{and} \quad x^3 + (\theta - p)\, x^2y + \dots,$$

which in the field $K(\theta)$ can have only a finite number of ideal factors in common. Hence we have the equation in ideals

$$(x - \theta y) = \lambda T^2,$$

where λ is one of a finite number of ideals and T is an ideal. As the number of ideal classes is finite, we can put

$$T = uv,$$

where v is an algebraic number given by

$$nv = a + b\theta + c\theta^2 + d\theta^3 \text{..................(8a)},$$

with a, b, c, d integers, while u and n are a pair taken from a finite number of ideals and ordinary integers respectively. Hence

$$(x - \theta y) = \lambda u^2 v^2.$$

But all the units in the field $K(\theta)$ can be written in the form $U_1 U_2^2$ where U_1, U_2 are units, for a finite number of values of U_1. Hence as λu^2 must be a principal ideal, we have an equation of the form

$$x - \theta y = \sigma v^2 / M \text{ ....(9)},$$

where M is one of a finite number of ordinary integers, σ one of a finite number of algebraic integers, and v is an algebraic number of the form (8 a). Some of the equations (9) may supply only a finite number of values of x, y, v; but if the equation (8) has an infinite number of solutions, one of the equations (9) will also give an infinite number of values for x, y, v. Hence we have for a particular set x_0, y_0, v_0, and there are only a finite number of such sets required,

$$M(x_0 - \theta y_0) = \sigma v_0^2.$$

We may also suppose that x_0, y_0 is the smallest set satisfying this equation, reckoning the magnitude of sets from the maximum value of $|x_0|, |y_0|$. Hence we can deduce an equation of the form

$$M^2 (x - \theta y)(x_0 - \theta y_0) = (A + B\theta + C\theta^2 + D\theta^3)^2 \text{ ...(10)},$$

which has an infinite number of integer values of x, y, A, B, C, D, where the integers M, x_0, y_0 are selected from a finite set. We can also deduce such an equation if (9) is satisfied by two sets of values. If (9) is satisfied by only one set, we can call it an isolated set.

The success of my investigation depends upon the fact that from equation (10), x and y can be expressed rationally in terms of a new solution z_1, x_1, y_1 of equation (8), where x_1, y_1 are practically linear functions of A, B, C, D. Moreover, by considering the three equations conjugate to equation (10), it is clear that*

$$A,\ B,\ C,\ D = O\ [\max |x|^{\frac{1}{2}},\ |y|^{\frac{1}{2}}]$$

and that the same result holds for $x_1, y_1, \ldots$. From a sequence

$$|\xi_n| < \kappa |\xi_{n-1}|^{\frac{1}{2}},\quad |\xi_{n-1}| < \kappa |\xi_{n-2}|^{\frac{1}{2}}, \ldots |\xi_1| < \kappa |\xi_0|^{\frac{1}{2}}$$

we have (if $\kappa > 1$) $$|\xi_n| < \kappa^2 |\xi_0|^{1/2^n},$$

so that the method of infinite descent applies, that is, by applying the same process to $x_1 y_1$, we deduce solutions $x_2 y_2$, $x_3 y_3 \ldots$ until we come to a solution $x = x_n$, $y = y_n$, which either cannot be expressed in the form (10), or if it can, leads to a solution identical with x_n, y_n; or which will be a solution of an equation (9), that is x_n, y_n will be either a minimum set or an isolated set. Hence x, y can be expressed rationally in terms of a finite number of solutions $x_1 y_1 z_1$, $x_2 y_2 z_2, \ldots x_n y_n z_n$.

§ 5. To simplify the algebra, consider first the case when

$$(x - \theta y)\,\theta = (a + b\theta + c\theta^2 + d\theta^3)^2 \;\ldots\ldots\ldots\ldots(11),$$

and $$\theta^4 = p\theta^3 + q\theta^2 + r\theta + s,$$

corresponding to the solution for which $x_0 = 0$.

The square of the right-hand side is

$$a^2 + 2ab\theta + (b^2 + 2ac)\,\theta^2 + 2\,(bc + ad)\,\theta^3 + (c^2 + 2bd)\,\theta^4 + 2cd\theta^5 + d^2\theta^6.$$

Also $$\theta^5 = p\theta^4 + q\theta^3 + r\theta^2 + s\theta,$$

$$\theta^6 = p\,(p\theta^4 + q\theta^3 + r\theta^2 + s\theta) + q\theta^4 + r\theta^3 + s\theta^2.$$

Hence equating coefficients of θ^0, θ^3 on both sides of (11),

$$a^2 + s\,(c^2 + 2bd + 2cdp + d^2p^2 + d^2q) = 0,$$

$$2ad + 2bc + 2cdq + d^2\,(pq + r) + p\,(c^2 + 2bd + 2pcd + d^2p^2 + d^2q) = 0.$$

This result still holds when the quartic has two irreducible quadratic factors, as equation (11) is true if θ is the root of either quadratic. Eliminating b between these equations by multiplying the first equation by $c + pd$, the second by $-sd$ and adding, we have on arranging the result in powers of a,

$$(c + pd)\,a^2 - 2asd^2 + (c + pd)\,(s\,[c + pd]^2 + qsd^2)$$
$$- s\,(d^3\,[p^3 + pq] + d^3\,[pq + r] + 2cd^2\,[p^2 + q] + c^2dp) = 0.$$

* The bracket refers to the greater of $|x|^{\frac{1}{2}}$, $|y|^{\frac{1}{2}}$.

Put now $c+pd=\rho$, and this becomes

$$a^2\rho-2asd^2+s\rho^3-psd\rho^2-qsd^2\rho-srd^3=0,$$

whence $$a\rho=sd^2\pm[-s(\rho^4-p\rho^3d-q\rho^2d^2-r\rho d^3-sd^4)]^{\frac{1}{2}}.$$

Also from equation (11), by changing θ into its conjugate values and multiplying the resulting equations together

$$-s(x^4-px^3y-qx^2y^2-rxy^3-sy^4)=z^2 \text{ say } \quad \ldots\ldots(12).$$

It is also clear that

$$a, b, c, d, \rho=O\,[\,|\,x\,|^{\frac{1}{2}}, |\,y\,|^{\frac{1}{2}}],$$

and that as b and also x, y from (11) are rationally expressed in terms of a, ρ, d, the solution x, y of (12) is expressed in terms of another solution ρ, d of (12). Hence the method of infinite descent applies, as we can continue the process with the solution ρ, d first removing their common factors, until we come to a solution, say x_n, y_n which either cannot be expressed in the form (11), that is (10) with $x_0=0$, or if it can, leads to a solution

$$x_{n+1}=x_n,\quad y_{n+1}=y_n.$$

So we now consider the case wherein we do not take $x_0=0$.

We turn then to equation (10), namely

$$M^2(x-\theta y)(x_0-\theta y_0)=(A+B\theta+C\theta^2+D\theta^3)^2 \ldots(10),$$

and put $$x_0-\theta y_0=\phi,$$

where we note $y_0=0$ is excluded, since a in equation (8) is not a perfect square. The resulting equation takes the form

$$(X-\phi Y)\,\phi=(a_1+b_1\phi+c_1\phi^2+d_1\phi^3)^2 \quad \ldots\ldots(12\text{a}),$$

say, where now

$$\phi^4-p_1\phi^3-q_1\phi^2-r_1\phi-s_1=0.$$

Hence X, Y and so x, y are rationally expressible in terms of

$$\rho_1, d_1 \text{ and } [-s_1(\rho_1{}^4-p_1\rho^3d_1\ldots)]^{\frac{1}{2}},$$

where $\rho_1=c_1+p_1d_1$.

But since

$$\left(\frac{x_0-\phi}{y_0}\right)^4-p\left(\frac{x_0-\phi}{y_0}\right)^3-\ldots=\frac{1}{y_0{}^4}(\phi^4-p_1\phi^3\ldots),$$

we have on equating terms independent of ϕ

$$az_0{}^2=x_0{}^4-px_0{}^3y_0-qx_0{}^2y_0{}^2\ldots=-s_1.$$

Replacing also ϕ by ρ_1/d_1 and putting

$$\frac{\rho}{d}=\frac{x_0-\rho_1/d_1}{y_0}=\frac{d_1x_0-\rho_1}{d_1y_0},$$

so that
$$\rho = \frac{1}{\lambda}(d_1 x_0 - \rho_1), \quad d = \frac{1}{\lambda} d_1 y_0,$$
where λ is taken so that the integers ρ and d are prime to each other, we have
$$\rho^4 - p\rho^3 d - q\rho^2 d^2 \ldots = \frac{1}{y_0{}^4}(\rho_1{}^4 - p_1\rho_1{}^3 d_1 \ldots)\left(\frac{d}{d_1}\right)^4.$$
Hence x, y are rationally expressible in terms of
$$\rho, d \text{ and } [a[\rho^4 - p\rho^3 d \ldots]]^{\frac{1}{2}},$$
so that not only are ρ, d another solution x, y of equation (8), but as practically linear functions of d_1, ρ_1, and hence of A, B, C, D, they are
$$O\,[\max |x|^{\frac{1}{2}},\ |y|^{\frac{1}{2}}],$$
as is clear from the equation (10) and the conjugate equations.

Hence the method of infinite descent applies, so that all the solutions x, y, z of (8) can be expressed rationally in terms of a finite number
$$x_1, y_1, z_1;\ x_2, y_2, z_2;\ \ldots\ x_n, y_n, z_n, \ldots;$$
or rather as the method of reduction leads to solutions wherein x, y, z may have a common factor, the theorem really applies to the ratios $\frac{x}{y}$, $\frac{z}{y}$, that is, to all the rational solutions of the equation
$$\eta^2 = a\xi^4 + b\xi^3 + c\xi^2 + d\xi + e \quad \ldots\ldots\ldots\ldots(13),$$
where the right-hand side has no rational linear factors in ξ.

§ 6. To interpret this result geometrically put $\eta = z_1/x_1{}^2$, $\xi = x_1/y_1$ and suppose that equation (8) takes the form (13). The solutions $x_1, y_1, z_1, \ldots x_n, y_n, z_n$, correspond to rational points $P_1, P_2, \ldots P_n$ on the curve. Then we have the theorem: all the rational points can be found by finding the intersection P_{n+1} with the curve of parabolas
$$\eta = L\xi^2 + M\xi + N \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(14)$$
passing through, say, the point P_1, and having double contact with the quartic at P_2 or P_1, and then continuing the process, including now P_{n+1}, among the points $P_1, P_2, \ldots P_n$, etc.

A simple way of proving this is to start from equation (11), change θ into $1/(\theta - \kappa)$, so that now $x_0 = 1$, $y_0 = 0$,
$$x - \theta y = (a + b\theta + c\theta^2 + d\theta^3)^2,$$
and by selecting κ properly we have
$$\theta^4 = q\theta^2 + r\theta + s.$$

Expanding and equating coefficients of θ, θ^2, etc., we find

$$bd = c^2 - qd^2 \pm (c^4 - qc^2d^2 - rcd^3 - sd^4)^{\frac{1}{2}},$$

$$2ad^2 = -2c^3 - rd^3 \mp 2c\,(c^4 - qc^2d^2 - rcd^3 - sd^4)^{\frac{1}{2}},$$

$$\frac{x}{y} = -\frac{a^2 + s\,(c^2 + 2bd + d^2q)}{2ab + r\,(c^2 + 2bd + d^2q) + 2cds} \;\ldots\ldots\ldots\ldots(15).$$

Put now $\xi = x/y$, take $d = 1$, and put

$$\kappa^2 = c^4 - qc^2 - rc - s.$$

We shall now show that a parabola of the form (14) drawn through the point $\xi = \infty$, $\eta = +\infty$ of the curve

$$\eta^2 = \xi^4 - q\xi^2 - r\xi - s \;\ldots\ldots\ldots\ldots\ldots\ldots(16),$$

to have double contact with it at the point $\xi, \eta = c - \kappa$, will meet it again in a point whose ξ coordinate is given by (15).

For changing the origin to $\xi = c$, $\eta = 0$, the quartic (16) becomes

$$\eta^2 = \xi^4 + A\xi^3 + B\xi^2 + C\xi + \kappa^2,$$

where $A = 4c$, $B = 6c^2 - q$, $C = 4c^3 - 2qc - r$.

The required parabola is then

$$\eta = \xi^2 - \frac{C}{2\kappa}\,\xi - \kappa,$$

and its fourth point of intersection with the quartic is given by

$$A\xi + B = -\frac{C}{\kappa}\,\xi + \frac{C^2}{4\kappa^2} - 2\kappa,$$

or
$$\xi = \frac{C^2 - 8\kappa^3 - 4\kappa^2 B}{4\kappa\,(A\kappa + C)}.$$

Also the expression (15) diminished by c, say ξ_1, is equal to ξ for

$$\xi_1 = -\frac{a^2 + s\,(c^2 + 2b + q)}{2ab + r\,(c^2 + 2b + q) + 2cs} - c,$$

where
$$b = c^2 - q + \kappa,$$
$$2a = -2c^3 - r - 2c\kappa,$$

on taking $d = 1$ as the equations are homogeneous in a, b, c, d Hence the denominator of ξ_1 becomes

$$-2c^5 + 2qc^3 + rc^2 + qr + \kappa\,(-4c^3 + 2cq - r) - 2c\kappa^2$$
$$+ rc^2 + qr + 2cs,$$

or
$$-2c\kappa^2 - 2c\kappa^2 + \kappa\,(-C),$$

or
$$-\kappa\,(A\kappa + C).$$

The numerator is

$$\begin{aligned}&c^6+c^3r+\tfrac{1}{4}r^2+(2c^4+cr)\,\kappa\\&c^6-qc^4-rc^3-sc^2+qs\\&\qquad\qquad -sc^2\\&\qquad\qquad +2c^2s-2qs+2\kappa s,\end{aligned}$$

or $$2c^6-qc^4+2sc^2-qs+\tfrac{1}{4}r^2+(2c^4+cr+2s)\,\kappa.$$

Hence $$\xi_1=\frac{\left\{\begin{matrix}2c^6-qc^4+2sc^2-qs+\tfrac{1}{4}r^2+(2c^4+cr+2s)\,\kappa\\-4c^2(c^4-qc^2-rc-s)\qquad-(4c^4-2qc^2-rc)\,\kappa\end{matrix}\right\}}{\kappa\,(A\kappa+C)}.$$

Also

$$\begin{aligned}\tfrac{1}{4}(C^2-8\kappa^3-4\kappa^2B)&=-2\kappa^3-(6c^2-q)(c^4-qc^2-rc-s)+(2c^3-qc-\tfrac{1}{2}r)^2\\&=-2\kappa^3-2c^6+3qc^4+4rc^3+6c^2s-sq+\tfrac{1}{4}r^2,\end{aligned}$$

which is the same as the numerator of ξ_1. Hence $\xi=\xi_1$ which proves the statement.

For the analytic interpretation we must turn to § 2 and consider the birational transformation between x, y, or using now ξ, η for them, and s, t, or u. Then corresponding to the point $\xi=\infty$, $\eta=+\infty$ we have $s=-c$, $t=d$, or, say, u_0, and to the point ξ, η, where the parabola touches the quartic, we have, say, the point u_1. Hence by the elementary properties of periodic functions

$$u_0+u+2u_1\equiv 0 \qquad (\text{mod } \omega_1,\ \omega_2).$$

Similarly operating on u_1, we have

$$\begin{aligned}v_0+u_1\quad+2u_2&\equiv 0,\\w_0+u_2\quad+2u_3&\equiv 0,\\&\cdots\cdots\cdots\cdots\\k_0+u_{n-1}+2u_n&\equiv 0,\end{aligned}$$

and, repeating this process, we can express u in terms of the quantities u_0, v_0, w_0, ..., which are finite in number, the previous work showing that the process finishes by coming to a stage where $u_n=u_0$, or v_0, or w_0, etc. Hence we have

$$u+u_0-2v_0+2^2w_0\ldots\pm 2^nu_n=0.$$

Now every integer can be represented in the scale 2 in the form

$$\pm 1\pm 2\pm 2^2\pm 2^3\ldots,$$

the signs being independent of each other. Hence, as the u_0, v_0, ... need not be all different, we have

$$u=m_1\xi_1+m_2\xi_2+\ldots m_n\xi_n,$$

where m_1, m_2, ... m_n are any integers negative, positive, or zero,

n is finite, and $\xi_1, \xi_2, \ldots \xi_n$ are n given quantities corresponding to n values of u. A more symmetrical notation is

$$u = m_1 u_1 + m_2 u_2 \ldots + m_n u_n.$$

§ 7. We must still discuss the case when the quartic (8) has a rational linear factor, so that a solution of equation (8) is at hand with $z = 0$. Hence from § 2, all that we require is the complete solution of the equation

$$t^2 = 4s^3 - g_2 s - g_3 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(3),$$

supposed to have an infinite number of rational solutions.

Suppose first of all that there is a binary quartic in x, y with invariants g_2, g_3, without rational linear factors, which becomes a perfect square for one value of x, y, and hence from § 2 for an infinite number of values of x, y. From § 2 the values of x, y are expressed in terms of $s = \wp(u)$, $t = \wp'(u)$ and from § 6 the general value of u is known. Hence the general solution of equation (3) is given by

$$s = \wp(m_1 u_1 + \ldots m_n u_n), \quad t = \wp'(m_1 u_1 + \ldots m_n u_n),$$

where the quantities $u_1, u_2, \ldots u_n$ are finite in number and $m_1, m_2, \ldots m_n$ are any integers, positive, negative, or zero.

Next consider the case when no such quartic exists. Multiplying equation (3) throughout by 16, we see there is no loss of generality in putting

$$g_2 = 4G_2, \quad g_3 = 4G_3,$$

where G_2, G_3 are integers, and considering the equations

$$t^2 = s^3 - G_2 s - G_3.$$

Writing now $s = x/y$ with x prime to y, we can put

$$z^2 = y(x^3 - G_2 x y^2 - G_3 y^3).$$

Hence both factors on the right hand are perfect squares, so that* by § 3 we can put

$$x = H(x_1, y_1), \quad y = F(x_1, y_1), \ \ldots\ldots\ldots\ldots(16\text{ a})$$

where F is a representative of the classes of binary quartics with invariants $4G_2, 4G_3$. By hypothesis F has a rational linear factor, so that we can suppose F is given by

$$y_1(4Bx_1^3 + 4Dx_1 y_1^2 + E_1 y_1^3).$$

* We have an infinite number of quartics (included among a finite number of classes) invariants $4G_2$, $4G_3$ with first coefficient y^2, but it does not seem easy to prove these have no rational linear factors.

On writing down the condition that its invariants are $4G_2$, $4G_3$, this takes the form

$$y_1\left(4bx_1^3 - \frac{4G_2}{b}x_1y_1^2 - \frac{4G_3}{b^2}y_1^3\right) \quad \text{............(17)},$$

where b has a finite number of integer values.

Hence $$y_1[(bx_1)^3 - G_2(bx_1)y_1^2 - G_3y_1^3]$$

is a perfect square, and x_1, y_1 are prime to each other since x is prime to y. If b and y_1 have a common factor κ, put

$$y_1 = \kappa Y, \quad b = \kappa B,$$

then $$Y[(Bx_1)^3 - G_2(Bx_1)Y^2 - G_3Y^3]$$

is a perfect square, and now Y is prime to Bx_1. Hence

$$Bx_1 = h(x_2, y_2), \qquad Y = f(x_2, y_2),$$

or $$bx_1 = \kappa h(x_2, y_2), \quad y_1 = \kappa f(x_2, y_2)$$

where f is again a binary quartic with invariants $4G_2$, $4G_3$, which must also be of the form (17) with not necessarily the same b.

Now* $$x_1, y_1 \text{ are } O\,[\max |x|^{\frac14}, \quad |y|^{\frac14}],$$

$$x_2, y_2 \text{ are } O\,[\max |x_1|^{\frac14}, \quad |y_1|^{\frac14}],$$

so that the method, etc., of infinite descent applies and we must arrive at a finite number of solutions, in terms of which all the others can be expressed. Moreover, if we put

$$x/y = \wp(u), \quad bx_1/y_1 = \wp(u_1),$$

we have $u = 2u_1$†, showing that the same rule holds as before.

§ 8. Finally we consider the case of the homogeneous ternary cubic of genus one, which we write as

$$f(x, y, z) = 0.$$

If this equation has an infinite number of integer solutions, we first of all apply a linear transformation

$$x, y, z = L(\xi, \eta, \zeta),$$

so that the coefficient of ζ^3 is zero in the new equation, which then becomes

$$\zeta^2S_1 + 2\zeta S_2 + S_3 = 0 \quad \text{..................(18)},$$

where S_1, S_2, S_3 are binary linear, quadratic and cubic forms in ξ, η.

Hence $$\zeta S_1 = -S_2 \pm (S_2^2 - S_1S_3)^{\frac12}.$$

* This follows from (16a) as $x_1 - ey_1$ is the square of a quadratic function of x, y for three values of e.

† See my paper "The inversion of the integral, etc." *Messenger of Mathematics*, vol. 43, 1915, page 140.

The radical is now a binary quartic in ξ, η. Hence ξ, η and so ζ can be rationally expressed in terms of a finite number of solutions, say, $\xi_1, \eta_1; \xi_2, \eta_2 \ldots \xi_n, \eta_n$. Hence any solution x, y, z can be rationally expressed in terms of a finite number of solutions $x_1, y_1, z_1; x_2, y_2, z_2, \ldots x_n, y_n, z_n$; or, more accurately, this is the time for the ratios x/z, y/z in terms of x_1/z_1, y_1/z_1, etc.

Moreover, the method of derivation is the classical one in § 1. For a linear transformation

$$\xi', \eta' = L_1(\xi, \eta), \quad \zeta' = \zeta + a\xi + b\eta$$

reduces the cubic (18) to the form

$$\zeta^2\eta - \zeta\xi^2 + S_3 = 0,$$

so that
$$2\zeta\eta = \xi^2 \pm (\xi^4 - S_3\eta)^{\frac{1}{2}}.$$

Another substitution

$$\xi' = \xi + k\eta, \quad \zeta' = \zeta + A\xi + B\eta$$

gives
$$2\zeta\xi = \xi^2 + c\eta^2 \pm (\xi^4 + 6c\xi^2\eta^2 + 4d\xi\eta^3 + e\eta^4)^{\frac{1}{2}},$$

which is the birational transformation considered in § 2. Hence we can take

$$\frac{\zeta}{\eta} = \wp(u), \quad \frac{\xi}{\eta} = \frac{\wp'(u) - \wp'(u_0)}{\wp(u) - \wp(u_0)},$$

where from § 6 the general value of u is given by

$$u = m_1u_1 + m_2u_2 \ldots + m_nu_n$$

where $m_1, m_2, \ldots m_n$ are any integers positive, negative or zero, and $u_1, u_2, \ldots u_n$ are finite* in number. Also the parameters v_1, v_2, v_3 of three collinear points on the cubic satisfy the equation

$$v_1 + v_2 + v_3 + u_0 \equiv 0 \quad (\text{mod } \omega_1, \omega_2).$$

Hence the result follows.

In conclusion, I might note that the preceding work suggests to me the truth of the following statements concerning indeterminate equations, none of which, however, I can prove. The left-hand sides are supposed to have no squared factors in x, the curves represented by the equations are not degenerate, and the genus of the equations is supposed not less than one.

(1) The simultaneous indeterminate equations

$$ax^4 + bx^3 + cx^2 + dx + e = y^2,$$
$$a_1x^4 + b_1x^3 + c_1x^2 + d_1x + e_1 = y_1^2$$

can be satisfied by only a finite number of *rational* values of x.

* u_0 is included amongst them.

(2) The equation

$$ax^4 + bx^3 + cx^2 + dx + e = y^2$$

can be satisfied by only a finite number of *integral* values of x: and the same theorem holds for

$$ax^n + bx^{n-1} \dots kx + l = y^2.$$

(3) The equation

$$ax^6 + bx^5y + \dots fxy^5 + gy^6 = z^2$$

can be satisfied by only a finite number of *rational* values of x and y with the obvious extension to equations of higher degree.

(4) The same theorem holds for the equation

$$ax^4 + by^4 + cz^4 + 2fy^2z^2 + 2gz^2x^2 + 2hx^2y^2 = 0.$$

(5) The same theorem holds for any homogeneous equation of genus greater than unity, say, $f(x, y, z) = 0$.

It may be noted that if $f = 0$ represents a curve of genus unity, all of its rational points can be expressed rationally by means of a finite number of them; since Poincare has proved* that $f = 0$ can be transformed into a cubic by a birational transformation with rational coefficients.

* *Journal de Mathématique*, 5th series, vol. VII, 1901, page 177.