COMPLETE GROUPS OF POINTS ON A PLANE CUBIC CURVE OF GENUS ONE*

BY

M. I. LOGSDON

1. Of the great number of papers which have been published which deal with rational solutions of cubic equations in two non-homogeneous or three homogeneous variables, the majority have been concerned with special numerical examples. (See Dickson's *History of the Theory of Numbers,* vol. 2, 1920, Chap. 21, for an account of these papers.) Some few, however, have dealt with the general problem of classifying cubics with rational coefficients with reference to rational solutions. Of these, the following have been consulted in the preparation of this paper:

B. Levi, *Atti,* IV *Congresso Internazionale Matematico,* Roma, vol. 2, 1909, pp. 173-7.

B. Levi, Atti, Reale Academia delle Scienze, Torino, vol. 41 (1906), pp. 739-64; vol. 43 (1908), pp. 99-120; 413-434; 672-681.

A. Hurwitz, Vierteljahrschrift der Naturforschenden Gesellschaft, Zürich, vol. 62 (1917), pp. 207-229.

H. Poincaré, Journal de Mathématiques, ser. 5, vol. 7 (1901), pp. 161-204.

L. J. Mordell, Proceedings of the Cambridge Philosophical Society, vol. 21 (1922), pp. 181-6.

L. J. Mordell, Science Progress, London, July, 1923.

If there is a known rational point on the cubic curve, the graph of

$$f(x, y, z) = 0, \tag{1}$$

where $f(x, y, z)$ is homogeneous of degree three in the variables, other rational points may be found from this one by drawing tangents and secants. Hurwitz, in the paper quoted, page 207, calls this the *fundamental construction* and the group of points consisting of all that may be thus obtained from a given *basis* he calls a *complete group.* (A definition of basis as used by Levi will be given in § 3.)

The *anharmonic ratio of a cubic of genus one* is by definition the anharmonic ratio of the pencil of four tangents to the curve from any point on it. This ratio is independent of the point from which the tangents are drawn.†

In this paper a study is made of the geometrical configurations of rational points obtained by the fundamental construction from one or more

* Presented (in part) to the Society, December 29, 1922.

† Salmon, *Higher Plane Curves,* 3d edition, 1879, p. 144.

known rational points on cubics of genus one with *rational anharmonic ratio,* with a very brief summary of known results in the case of genus zero.

2. If the genus of the cubic is zero, in fact for the general equation $f(x, y, z) = 0$, of degree n with rational coefficients and genus zero, the problem of classification and solutions has been completely solved. By a succession of birational transformations a set of equations can be obtained,

$$\begin{aligned} f = f_0 &= 0, \\ f_1 &= 0, \\ f_2 &= 0, \\ &\cdots\cdots, \end{aligned}$$

each of degree two less than the one which precedes it in the set, but equivalent to it in the sense that to every rational solution of $f_i = 0$ $(i = 1, 2, \cdots)$ will correspond a uniquely determinable rational solution of f_{i-1} and hence of the original equation, while conversely every solution (rational) of the given equation is obtainable from those of $f_1 = 0$, $f_2 = 0$, etc. with the possible exception of the $(n-1)(n-2)/2$ double points. These latter are the fundamental points of the transformations and can always be found by solving a finite number of algebraic equations. If n is odd the final equation of the set is linear and consequently has an infinite number of rational solutions, while if n is even, say $n = 2k$, after $k-1$ steps a quadratic equation is obtained. This will have no rational solutions or an infinite number. The test is (Legendre) as follows:

If in the conic $ax^2 + by^2 + cz^2 = 0$ the a, b, c are relatively prime in pairs, a situation always obtainable by the transformation

$$\begin{aligned} x' &= mx, \\ y' &= ny, \\ z' &= pz, \end{aligned}$$

there will be one and hence an infinity of solutions if and only if a, b, c, are not all of the same sign and $-bc$, $-ca$, $-ab$ are quadratic residues of a, b, c respectively. If there are no rational solutions to the quadratic equation the original $f = 0$ has no rational solutions other than *possibly* the douple or multiple points finite in number and obtainable as simultaneous solutions of $f_x = 0$, $f_y = 0$, $f_z = 0$, the three left members designating the three partial derivatives of f. In either case the inverses of the transformations used enable us to express all the rational solutions of $f = 0$ if infinite in number rationally in terms of a rational parameter.*

* Cf. Hilbert and Hurwitz, Acta Mathematica, vol. 14 (1890-91), pp. 217-24.

3. If the genus is unity, the coördinates of points on the cubic, C, defined by (1) where $f(x, y, z)$ is a cubic ternary form with rational coefficients are expressible in terms of an elliptic parameter. The *tangential** of a known rational point, P_0, will be the third point of intersection with the cubic of the tangent

$$xf_{x_0} + yf_{y_0} + zf_{z_0} = 0 \tag{2}$$

at P_0. If two rational points are known and neither is the tangential of the other, the secant line joining the two will cut the cubic in a third rational point. If after a finite number of operations, no new points can be obtained by this construction, we say we have a complete group of rational points. There will be a finite number of points in a complete group.

It will be shown that a certain choice of coördinate representation will assure the presence of an inflexion point among the points of a complete group. If besides the inflexion point there are r points which with the inflexion have the property that all and only the points of the group may be obtained from them by the fundamental construction, the r points are called the *basis* of the group. This definition of basis is due to Levi.† It differs from that of Poincaré in that by excluding an inflexion from the r points rank becomes invariant. Thus a cubic with only one rational point is of *rank* zero (see next sentence), since the cubic is birationally equivalent to a cubic with a rational inflexion and no other rational point.

If a complete group exhausts the rational points of the cubic, its basis, r, is called the *rank* of the cubic. If there should be more than one complete group on a cubic having the respective bases $r_1, r_2, \cdots$, and no rational points not in these groups, the rank of the cubic is defined as $r_1 + r_2 + \cdots = r$. Whether there can be more than one complete group on a cubic is a question which has not been answered. That rank is finite was proved by Mordell in the 1914 paper cited. The notion of rank may be extended to a cubic with an infinite number of rational points. If there are r points which have the property that from them and the rational inflexions in complete groups, if any are present, may be obtained by the fundamental construction all of the rational points of the cubic, r is called again the rank of the cubic.

4. If only a finite number of points may be obtained from a known rational point, A_0, by the fundamental construction, the same is true if the process of finding tangentials only is used. Let $A_0, A_1, A_2, \cdots, A_{k-1}$ be rational points on C, let A_i be the tangential of A_{i-1} $(i = 1, 2, \cdots, k)$, and let α_i be the elliptic argument of the point A_i,

* J. J. Sylvester, American Journal of Mathematics, vol. 3 (1880), pp. 61-66.

† Loc. cit. vol. 41 (1906), p. 758.

$$\alpha_i = \int_0^{\mu_i} \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}; \tag{3}$$

then, since the sum of the arguments of three collinear points on C is divisible by a period we have

$$\alpha_i \equiv -2\alpha_{i-1} \qquad \text{(modulo a period).}$$

The set of A's may terminate in either of two ways. A point A_k may be reached ($k = 0, 1, 2, \cdots, k$), which is an inflexion point or the point A_k may coincide with one of the points $A_i (0 \leqq i \leqq k-3)$ previously obtained. The geometric configurations consisting of these $k+1$ points are called by Levi (loc. cit., vol. 43 (1898), p. 101) *arborescent* and *polygonal* respectively. In the latter case there will be a closed polygon of $k-i$ vertices. In either case the argument, α, of the general point of the set is commensurable with a period of the Jacobi functions of α which will be used in representing the coördinates of the point A after equation (1) has been transformed to a normal form. (See § 10.)

For

$$\begin{aligned}
\alpha_1 &\equiv -2\alpha_0 && \text{(modulo a period),}\\
\alpha_2 &\equiv -2\alpha_1 \equiv (-2)^2\alpha_0 && \text{(modulo a period),}\\
\alpha_3 &\equiv -2\alpha_2 \equiv (-2)^3\alpha_0 && \text{(modulo a period),}\\
&\cdots\cdots\cdots\cdots\\
\alpha_{k-1} &\equiv -2\alpha_{k-2} \equiv (-2)^{k-1}\alpha_0 && \text{(modulo a period),}
\end{aligned}$$

and finally we have the respective cases

I. $$\alpha_k \equiv (-2)^k\alpha_0 = \omega_1/3 \text{ or } \equiv 0 \qquad \text{(modulo a period),}$$

depending on whether this particular point of inflexion corresponds to zero or not (the value of the elliptic parameter corresponding to any point of inflexion in any coördinate system will be zero or one third of a period), whence

$$\alpha_0 = \frac{\omega_1}{3\cdot 2^k} \text{ or } \omega_2/(-2)_k;$$

II. $$\alpha_k \equiv (-2)^k\alpha_0 \equiv (-2)^i\alpha_0;$$

whence

$$\alpha_0 = \frac{\omega_3}{(-2^k)-(-2)^i},$$

where ω_1, ω_2, ω_3 are notations used to designate a convenient period not divisible by two, otherwise the set would have terminated at most with A_{k-1}.

The last equation may be simplified by factoring the denominator. One factor will be $(-2)^i$, another $(-2-1)$, and the final factor, which we shall denote by M, is

$$[(-2)^{k-i-1}+(-2)^{k-i-2}+\cdots+(-2)+1], \tag{4}$$

a quantity not divisible by 2. If $k=i+3$, M will be 3. We have then, in the polygonal case, that the argument of one of the points, say A_0, in the configuration is given by

$$\alpha_0 = \frac{-\omega_3}{(-2)^i \cdot 3 \cdot M} = \frac{(-1)^{i+1}\omega_3}{2^1 \cdot 3 \cdot M}. \tag{4a}$$

Thus if in the construction or computation of tangentials we are halted by reaching an inflexion, the elliptic argument of any point, A, of the group may contain in the denominator *one* factor 3 or a power of 2, but no further factor, while, second, if the set ends by the closing of a polygon with $k-i \geqq 3$ sides there will also be in the denominator another factor, M, defined in (4) which, as is evident, is different from 3 unless $k-i=3$, when the denominator is $2^i 3^2$. Moreover there will be i points of the group which are not vertices of the closed polygon.

5. For the algebraic investigation of configurations of rational points on C, *we assume a known rational point,* which we call A_0. If A_0 is not an inflexion point, i. e. does not also satisfy the Hessian of $f(x, y, z)=0$, we can by a preliminary transformation transform C into an equivalent (in the sense of § 2) cubic with a rational inflexion. Find A_1, the tangential of A_0. If A_1 is not an inflexion call its tangential A_2. If A_2 is not an inflexion and its tangential is not an inflexion we discuss separately the two cases:

I. The tangential of A_2 is A_0,

II. The tangential of A_2 is distinct from A_0.

Take the three points A_0, A_1, A_2 as vertices of the new triangle of reference. The transformation may be written

$$T: \qquad x' : y' : z' :: A_0 A_1 : A_1 A_2 : A_2 A_0,$$

where by $A_0 A_1$, for example, is meant the linear function whose graph is the line through the two points A_0 and A_1. In the first case the equation of the cubic becomes

$$ay'^2x' + bx'^2z' + cz'^2y' + dx'y'z' = 0.$$

Now transform to new variables x, y, z by the Cremona transformation

$$x : y : z :: x'y' : z'^2 : z'x',$$

and get, apart from the factor yz^2 which does not count in the transformation,

$$ax^2y + bz^3 + cxy^2 + dxyz = 0, \tag{5}$$

which has inflexion points at (0, 1, 0), (1, 0, 0), and $(c, -a, 0)$. In the second case transformation T reduces the cubic to

$$ax'^2y' + bx'^2z' + cx'y'^2 + dy'z'^2 + ex'y'z' = 0,$$

which by the Cremona transformation

$$x : y : z :: x'^2 : x'y' : y'z' \tag{6}$$

becomes

$$axy^2 + bx^2z + cy^3 + dxz^2 + exyz = 0.$$

This has an inflexion at (0, 0, 1) with $x = 0$ as inflexion tangent. In both cases, the final cubic has rational coefficients.*

6. In view of the preceding we may henceforth assume that the equation

$$f(x, y, z) = 0 \tag{1}$$

is a homogeneous cubic with rational coefficients with a known rational solution and that this solution corresponds to an inflexion point, A_0, of the cubic curve C. By choosing the inflexion tangent for a new x-axis, any other line through A_0 for the y-axis, and the harmonic line of A_0 for the z-axis, a transformation with rational coefficients,† we get Newton's form of the cubic, viz.,

$$axz^2 + by^3 + cy^2x + dyx^2 + dx^3 = 0. \tag{7}$$

---

* That k^2 is invariant under linear transformation is well known. That it is also invariant under the Cremona transformations here employed is easily verified by the method of computation described in § 7.

† Since A_0 is a rational inflexion point, its quadratic polar will factor into two linear factors one of which will correspond to the inflexion tangent through A_0 and the second to a line not through A_0 called the harmonic line of A_0. With our present coördinate system the first factor representing the inflexion tangent has rational coefficients, hence the function corresponding to the harmonic line will also have rational coefficients. Cf. Salmon's *Higher Plane Curves*, 3d edition, 1879, p. 147.

On dividing by a, which obviously can not be zero, this becomes

$$xz^2 - g(y^3 + hy^2x + myx^2 + nx^3) = 0.$$

If the three roots of

$$y^3 + hy^2x + myx^2 + nx^3 = 0$$

are designated by r_1, r_2, r_3 each line $y - r_ix = 0$ is tangent to C at $z = 0$, whence the anharmonic ratio of the cubic is that of the pencil of tangents

$$x = 0,\ y - r_1x = 0,\ y - r_2x = 0,\ y - r_3x = 0,$$

and this is $(\infty r_3 r_2 r_1) = (r_3 - r_2)/(r_3 - r_1)$. If $r_1 + r_2 + r_3 = 3r_3$, this ratio is -1 and the cubic is harmonic. Geometrically this means that either (a) A_0 is the tangential of three real points all rational or one rational, whence the cubic consists of two branches, — an odd branch infinite in extent and an even branch or oval, or (b) one tangent from A_0 is real and the other two are imaginary, whence the cubic has only one real branch, the infinite one. Thus for all rational values of $k^2 = (\infty r_3 r_2 r_1)$ other than $k^2 = -1, 2, \frac{1}{2}, 0$ there will be three distinct real tangents from (0, 0, 1) to the cubic and the oval of the cubic will consist of real points.

In what follows we shall mean by C a cubic of genus one with rational anharmonic ratio different from $-1, 2, \frac{1}{2}, 0$ and for definiteness we assume $r_1 < r_2 < r_3$. Then k^2 will be a positive rational number less than unity.

7. The above discussion has shown that if a given cubic is transformed by the indicated steps to the form (7) the value of k^2 may be found at once. We shall show that for certain values of k^2 there will be on the curve four and no more rational points in a complete group, for certain other values of k^2 there will be exactly eight such points, while the presence of a ninth rational point assures an infinite number. It will then in general be desirable to have a method for computing k^2 without reducing (1) to canonical form, for since k^2 is invariant under the transformations we are using it will usually be simpler to compute k^2 from (1) for any particular cubic studied to see if it falls into one of the categories about which we can make definite statements.

Computation of k^2. The biquadratic which gives the four tangents from the known rational point, $A_0(x_0, y_0, z_0)$ not here assumed to be an inflexion, is given by*

* Salmon's *Higher Plane Curves*, 3d edition, 1879, p. 62.

$$\Delta^2 - 4\Delta' f = 0 \tag{8}$$

where $\Delta = x_0 f_x + y_0 f_y + z_0 f_z$ and $\Delta' = x f_{x_0} + y f_{y_0} + z f_{z_0}$. By solving (8) with a convenient one of the coördinate axes, we get the binary quadratic which gives the ratios of the four points of intersection of this axis with the four tangents which, by Pappus' theorem, gives the quantity we seek. The six values of the anharmonic ratio are the negatives of the ratios of the roots of

$$z^3 - 6iz - d = 0,$$

where $i = 2(a_0 a_4 - 4a_1 a_3 + 3a_2^2)$, $d^2 = 32(i^3 - 6j^2)$, and

$$j = 6\begin{vmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{vmatrix},$$

i and j being the invariants of the biquadratic whose coefficients are designated by $a_0, 4a_1, \cdots$, etc. If $i = 0$, $j \neq 0$, we will have $k^2 = -\omega$, where $\omega^3 = 1$, and the cubic is called *equianharmonic*. It has only one real branch. If $j = 0$, the cubic is *harmonic*.*

By applying to (7) the transformation

$$\begin{aligned} y' &= \sigma(y - r_3 x), \\ y' - x' &= \sigma(y - r_1 x), \\ y' - k^2 x' &= \sigma(y - r_2 x), \end{aligned}$$

whose inverse is

$$x : y : z :: -x'/(r_3 - r_1) : y' - r_3 x'/(r_3 - r_1) : z',$$

we get, dropping primes,

$$xz^2 - \alpha y(y - x)(y - k^2 x) = 0, \tag{9}$$

where $\alpha = g(r_3 - r_1)$. Furthermore, α may be assumed a positive integer without a square factor, since any square factor may be rationally absorbed by the z^2 and if α is negative the transformation

$$x : y : z :: -x' : y' - x' : z'$$

* See Salmon, loc. cit., p. 199, where however the notation is different and the plus sign which occurs in both equations should be a minus sign. See also Dickson's *Algebraic Invariants*, 1914, p. 55, and Clebsch-Lindemann, *Vorlesungen über Geometrie*, French edition, vol. 1, p. 297.

replaces (9) by

$$xz^2 + \alpha y(y-x)(y-k'^2x) = 0 \qquad k'^2 = 1-k^2,$$

i. e., k'^2 is positive and less than unity as was k^2.*

8. In the coördinate system corresponding to (9) the points of which the origin is tangential are $(1, 1, 0)$, $(1, k^2, 0)$, $(1, 0, 0)$, and as before, $0<k^2<1$. The coördinates of points (x, y, z) on C are proportional to

$$\text{(10)} \qquad \mathrm{sn}^3u : \mathrm{sn}\,u : \sqrt{\alpha}\,\mathrm{cn}\,u\,\mathrm{dn}\,u,$$

and the elliptic arguments of the four rational points already known to be on C may be taken to be

$$\text{(11)} \qquad \alpha_0 = 0, \quad \alpha_1 = \omega'/2, \quad \alpha_2 = (\omega+\omega')/2, \quad \alpha_3 = \omega/2,$$

corresponding respectively to the points

$$A_0(0, 0, 1), \qquad A_1(1, 0, 0), \qquad A_2(1, k^2, 0), \qquad A_3(1, 1, 0),$$

where ω is a real period and ω' a pure imaginary period. We see from the figure (p. 483) that the lines $y = 0$ and $y = k^2x$ are tangent to the even branch of the curve at the points with elliptic arguments $\omega'/2$ and $(\omega+\omega')/2$ respectively, while $y = x$ is tangent to the odd branch at the point with argument $\omega/2$. In fact the convention (11) and our choice of coördinate triangle enable us to represent points on the *odd* branch in terms of ω *alone* while points on the *even* branch are represented by $\lambda\omega + \omega'/2$ (λ real).†

From (9) and the last footnote we see that α is an arithmetic invariant of the cubic as was stated by B. Levi in the article cited. He further states in the paper read at the Rome Congress, page 176, that by birational transformation rational in k^2 we can always obtain the canonical form

$$xz^2 - y(y-x)(y-k^2x) = 0.$$

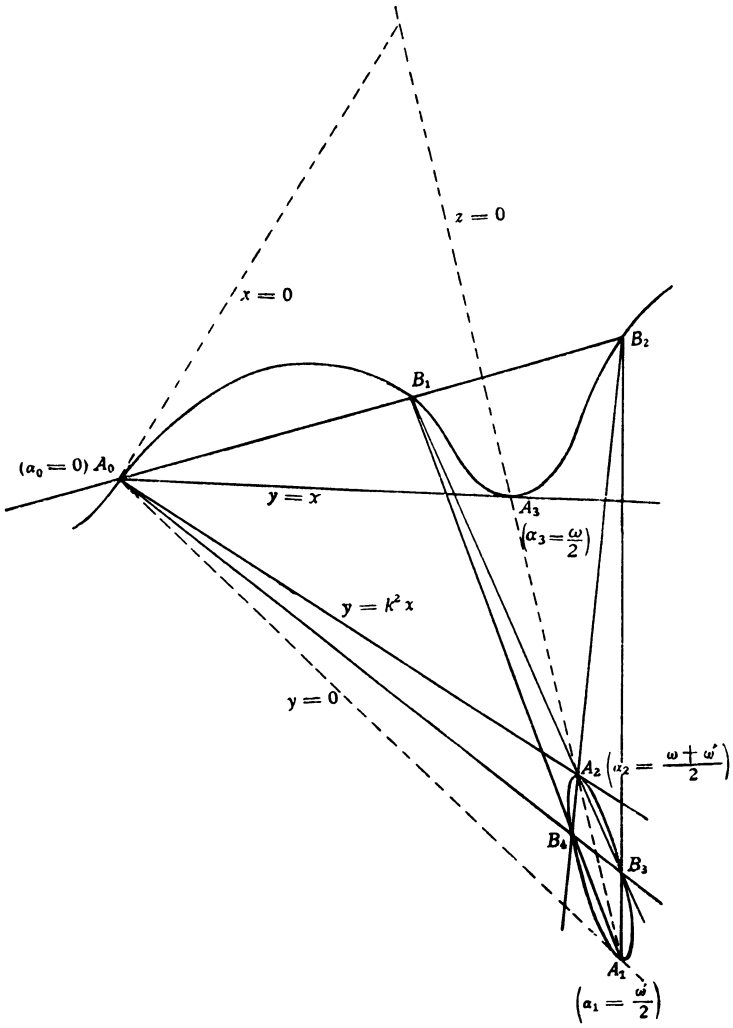
This is equivalent to the statement that two cubics with the same rational k^2 are birationally equivalent. That this is not the case is shown by the following example:

The equation $xz^2 - y(y-x)(y-3x/4) = 0$ has eight rational solutions, viz.: $(0, 0, 1)$, $(1, 0, 0)$, $(1, 1, 0)$, $(4, 3, 0)$, $(4, 6, \pm 3)$, $(4, 2, \pm 1)$,

* In fact, α is the numerical value of the largest non-square factor appearing in i^3/j^2; Levi, loc. cit., p. 751.

† Clebsch-Lindemann, loc. cit., p. 609-610.

while $xz^2 - 2y(y-x)(y-3x/4) = 0$ has only four rational solutions, the first four of the above list. Obviously the second equation is not birationally transformable into the first. This conclusion will follow also in § 9 from an analytical discussion of conditions under which the period is divisible.



We may summarize what has preceded thus:

THEOREM. *The equation* $f(x, y, z) = 0$ *of a plane cubic curve of genus unity, with rational anharmonic ratio,* $k^2 \neq 0$, *and with a known rational point, may by birational transformation with rational coefficients be brought to one of the forms*

$$\text{(i)} \qquad xz^2 - \alpha y(y^2 - yx + x^2) = 0, \quad k^2 = -1, \tfrac{1}{2}, 2;$$

$$\text{(ii)} \qquad xz^2 - \alpha y(y^2 + dx^2) = 0, \quad k^2 = -1, \tfrac{1}{2}, 2;$$

$$\text{(iii)} \qquad xz^2 - \alpha y(y - x)(y - k^2 x) = 0, \quad 0 < k^2 < 1, \ k^2 \neq \tfrac{1}{2},$$

where d is a rational number $\gtrless 0$, and α is a positive integer, containing no square factor. On the cubic there will be in the respective cases one, one or three, three groups of two rational points closed under the fundamental construction. Where there are three such two-groups they form a complete group of four points. The elliptic parameters of these rational points may be taken to be $0, \omega/2$ *and* $0, \omega/2, \omega'/2, (\omega + \omega')/2$ *where ω and ω' represent convenient real and pure imaginary periods. The rank will be one, one or two, two.*

9. Giving our attention now to the non-harmonic cubic with k^2 rational the question next arises: For what values of α and k^2 will there exist other rational points on C? If we solve

$$mx - \alpha y = 0$$

simultaneously with (9), in addition to the intersection at $A_0(0, 0, 1)$ we get the two intersections

$$\alpha : m : \pm\sqrt{m(m-\alpha)(m-k^2\alpha)}\,.$$

To find the solutions of

$$\text{(12)} \qquad m(m-\alpha)(m-k^2\alpha) = \text{a rational square}$$

we note that if the product of three quantities is a square, so is the quotient of any two of them by the third. Thus we shall have

$$\text{(13)} \qquad \begin{aligned} &(1) \quad m(m-\alpha) &&= (m-k^2\alpha)s^2, \\ &(2) \quad m(m-k^2\alpha) &&= (m-\alpha)s^2, \\ &(3) \quad (m-\alpha)(m-k^2\alpha) &&= ms^2, \end{aligned}$$

where α and k^2 are known constants, s is an arbitrary rational parameter, and any value of m which satisfies (12) will also satisfy the three equations (13). Thus the problem of finding all rational solutions of a cubic in m is replaced by the problem of finding all rational solutions of three quadratics in m. The m-discriminants of these equations must be squares different from zero. By making simple transformations the

discriminants may be reduced to the Pell equation $x^2 - Dy^2 = 1$ which will be satisfied in the respective cases by

$$(14)\quad \begin{aligned} &(1)\quad k^2 = \frac{(\alpha+s^2)^2-c^2}{4\alpha s^2}, && m = \frac{(\alpha+s^2)\pm c}{2},\\ &(2)\quad k^2 = \frac{(\alpha-c)s^2+c^2}{\alpha c}, && m = c \text{ or } \alpha s^2/c,\\ &(3)\quad k^2 = \frac{2(\alpha-s^2)}{\alpha}, && m = 2\alpha \text{ or } (\alpha - s^2), \end{aligned}$$

where s and c are arbitrary rational parameters, $\alpha > 0$ is an integer, k^2 is rational, positive and less than one.*

Each value of k^2 in (14) gives two distinct values for m and each value of m gives the two rational points on the curve

$$(15)\quad \alpha : m : \pm\sqrt{m(m-\alpha)(m-k^2\alpha)}.$$

For the respective values of k^2 these points will have for coördinates (the upper subscript is to be read with the upper sign):

(i) B_1 $\quad 4\alpha s : 2(\alpha+s^2+c)s : \pm(\alpha+s^2+c)(-\alpha+s^2+c)$,

B_3 $\quad 4\alpha s : 2(\alpha+s^2-c)s : \mp(\alpha+s^2-c)(\alpha-s^2+c)$;

(ii) B_1 $\quad \alpha : c : \pm s(c-\alpha)$,

B_3 $\quad c : s^2 : \pm s(s^2-c)$;

(iii) B_1 $\quad 1 : 2 : \pm 2s$,

B_3 $\quad \alpha : \alpha - s^2 : \pm s(\alpha - s^2)$.

* We may look upon the last paragraph thus: The normal form (9) of the cubic has two parameters, α and k^2. We seek all values k^2 which for a given α will assure the presence of a fifth rational point on the curve. Obviously, k^2 will be a function of α. If for any one of the equations (13) we could find all values of k^2 which would make the discriminant a positive square it would be unnecessary to consider the two remaining equations. However the way in which the parameters enter these discriminants has thus far made it impossible to be certain that all such expressions have been obtained, hence we use all three equations (13). Even so, no assertion is made as to the completeness with which the problem is solved, but it is true that if k^2 is expressible in any of the three forms (14), the cubic C in addition to the four rational points already found will have a fifth rational point, in fact will have at least four more rational points, as is shown in the next paragraph.

We next compute the tangentials of B_1, B_2, B_3, B_4 to see if, and under what conditions, the tangentials may coincide with points already found thus assuring that the group of eight points may be a complete group. In every case it is found that B_1 and B_4 have the same point for tangential, and that B_2 and B_3 have the same point for tangential. Calling these points B_{14} and B_{23} respectively, they are

(i) $B_{\substack{14\\23}}$ $8\alpha s^3 : 2(\alpha + s^2)^2 s : \pm c(\alpha + s^2)(\alpha - s^2)$,

(ii) $B_{\substack{14\\23}}$ $8\alpha s^3 c^3 : 2sc(s^2\alpha + c^2)^2 : \pm (s^2\alpha + c^2)(s^2\alpha - c^2)(2s^2 c - s^2\alpha - c^2)$,

(iii) $B_{\substack{14\\23}}$ $8s^3\alpha : 2s(s^2 + \alpha)^2 : \pm (s^2 + \alpha)(s^2 - \alpha)(3s^2 - \alpha)$.

Now since A_0, B_1, and B_2 are collinear; since A_0, B_3, and B_4 are collinear; and since A_0, B_{14}, and B_{23} are collinear, the only way in which B_{14} and B_{23} could coincide with any of the points previously found (thus completing an eight-group), would be for them to coincide simultaneously with A_1, or with A_2, or with A_3, each of which has the z-coördinate zero. Imposing this condition and remembering the previously assumed restrictions on α and k^2 we find that for $\alpha = 1$ in the first and second cases B_{14} and B_{23} coincide with A_3; k^2 is then $1 - c^2/4$ and $2c - c^2$ respectively, where c is any rational number with modulus < 2. For no other value of α is the eight-group closed. We state the

THEOREM. *If the numerical value of i^3/j^2 is a square, i. e., if i is a square and if one value of the anharmonic ratio of the cubic is a square less than unity, there will be on the cubic a complete group of eight points.*

If the invariants of the cubic are designated by S and T, from the relations $i^3/j^2 = -2^7 \cdot 3 \cdot S^3/T^2$ we can state the theorem thus:

THEOREM. *If the invariant S of the ternary cubic form $f(x, y, z) = 0$ is six times a square and if the cubic curve represented by $f = 0$ has anharmonic ratio one value of which is a positive rational square < 1, the curve will have a complete group of eight rational points.*

For all values of $\alpha \neq 1$ and values of k^2 given by (14) the preceding shows that there will be at least two additional rational points on C obtainable by the fundamental construction from the eight tabulated.

10. A study of the elliptic arguments of the points on the cubic furnishes the same *sufficient* conditions for the presence on the curve of a complete four-group or of a complete eight-group, together with the general

THEOREM. *If the tangential of the point B_1 coincides with A_3 there will be a complete eight-group on the cubic while in the contrary case there will be an infinite number of rational points on the cubic; in both cases all the*

rational points mentioned may be obtained from two of the group, one of A_1, A_2 *and one of* B_1, B_2, B_3, B_4. *The rank is two.*

In other words, if the elliptic argument corresponding to any one of the B's is an aliquot part of a primitive period* of the cubic, it will be one fourth of it, and the four B's will complete an eight-group, while if the elliptic parameter of B_1, say, does not divide a primitive period by four it will not divide it rationally and there will be an infinite number of rational points obtainable from these two by the fundamental construction. Proof of this theorem is in § 11.

The periods of the Jacobi elliptic functions are given by

$$4mK + 4m'iK',$$

where m and m' are positive or negative integers. Moreover $2K + 2iK'$ is a primitive period for the cubic, since an increase of u by $2K + 2iK'$ changes the sign of each of the three coördinates

$$\varrho \operatorname{sn}^2 u, \quad \varrho \operatorname{sn} u, \quad \varrho \sqrt{\alpha} \operatorname{cn} u \operatorname{dn} u.$$

Using the notation $\omega = 2K$, $\omega' = 2iK'$, and calling $\alpha_0, \alpha_1, \cdots, \beta_1, \beta_2, \cdots$ the arguments of $A_0, A_1, \cdots, B_1, B_2, \cdots$, we can by easy computation find that we may take

$$\alpha_0 = 0, \quad \alpha_1 = \omega'/2, \quad \alpha_2 = (\omega + \omega')/2, \quad \alpha_3 = \omega/2.$$

Since the sum of the elliptic arguments of three collinear points is congruent to zero modulo a period, if A_3 is to be the tangential of one and consequently of all four of the B's, the elliptic arguments of the latter points must be

(16) $\pm\frac{1}{4}\omega = \pm\frac{1}{2}K$ and $\pm\frac{1}{4}\omega + \omega'/2 = \pm\frac{1}{2}K + iK'$ (mod a period).

These are found to be (Cayley, loc. cit.)

(17) $1 : (1+k') : \pm\sqrt{\alpha}k'(1+k')$ and $1 : (1-k') : \mp\sqrt{\alpha}k'(1-k')$,

where k'^2 is the modulus conjugate to k^2. It is clear that these four ratios are real and rational if and only if k'^2 is a positive square and $\alpha = 1$. Referring to (14) and the results near the close of § 9, we find that k'^2 had the values $c^2/4$ and $(c-1)^2$, $|c| < 2$. Using these values

* See Cayley, *Elliptic Functions*, 2d edition, 1895, pp. 70 and 74.

in (16) we get numbers proportional to the coördinates of B_1, B_2, B_3, B_4 as given in the first tabulation after (15), as was to be expected. In any case the points whose arguments are given by (16) are on the cubic, since they satisfy (9) identically, but only if (1) $s^2 = \alpha = 1$, $k^2 = (4 - c^2)/4$, and (2) $\alpha = c^2/s^2 = 1$, $c = \pm s$, $k^2 = 2c - c^2$ will these points be rational and have A_3 as tangential, i. e. complete an eight-group.

11. We next enquire whether and under what conditions a group of points consisting of nine or more may close. In this case neither B_{14} nor B_{23} coincides with A_3. We construct the tangential of B_{14}, say. Call it N with argument ν;

$$\nu = -2\beta_{14} = 4\beta_1.$$

There are two cases to be considered:

(a) $\nu = K$, i. e. N coincides with A_3;

(b) $\nu \neq K$ and the tangential of N may be constructed.

In case (a),

$$\operatorname{sn}^2\beta_1 = \operatorname{sn}^2 \tfrac{1}{4}K = \frac{\sqrt{1+k'} - \sqrt{k'}}{\sqrt{1+k'}\,[1+\sqrt{k'}]}.$$

Now if the ratios $\operatorname{sn}^3\nu : \operatorname{sn}\nu : \sqrt{\alpha}\operatorname{cn}\nu\operatorname{dn}\nu$ are to be rational it will follow that $\operatorname{sn}^2\nu$ and $\sqrt{\alpha}\operatorname{sn}\nu\operatorname{cn}\nu\operatorname{dn}\nu$ must each be rational. Imposing these two conditions on ν we get for case (a) that $\nu = \frac{1}{4}K$ is a rational point if and only if

(1) k'^2 = positive rational square,

(2) $\alpha = 1$,

(3) $1 + k'$ = rational square.

But (1) and (2) are sufficient to assure a closed group of *eight* points. Hence, if B_{14} does not coincide with A_3 neither can its tangential, N.

In case (b), an easy induction shows that if B_{14} does not coincide with A_3, no point obtained by constructing successive tangentials from B_{14} can do so. The conditions will always include the ones obtained for case (a) above. In fact, the elliptic arguments of these successive tangentials, all obviously on the odd branch of the curve, will be $\pm 2^s\beta_1$, where $s = 1, 2, 3, \cdots$. If the sequence of points terminates in an inflexion, $\pm\frac{2}{3}K$, one of the points will have argument $\frac{1}{3}K$. The proof that these two points are not rational points on the cubic (9) is given in § 12. Also, if the sequence of points closes forming a polygon we shall have (see (4a), § 4)

$$2^s\beta_1 = \pm\frac{1}{2^i \cdot 3 \cdot M}K,$$

consequently some rational point of the group will have argument $(1/3M)K$.

We shall first show that in this case also the point with argument $\frac{1}{3}K$ must be in the group. For we can find positive integers $r, s, t, \cdots$ so that

$$M = 2^r \pm 2^s \pm 2^t \pm \cdots + 1$$

(see (4) in § 4), whence unless $M = 3$, by tangentials and secants we get that the rational point with argument

$$\beta = \frac{2^r \pm 2^s \pm 2^t \pm \cdots + 1}{3 \cdot M} K \tag{18}$$

is one of the points belonging to the complete group containing the vertices of the polygon. The exception occurs if $M = 3$, since in this case only the three vertices of the triangle, with arguments $\frac{2}{9}K$, $\frac{8}{9}K$, $\frac{14}{9}K$ (note: none of these is an inflexion) are obtained by tangentials and no additional points are obtained by secants. The proof is then complete with the following theorem:

12. *On the cubic* (9) *the real inflexion points with arguments* $\pm\frac{2}{3}K$ *are not rational points.*

Proof. By (18), $\beta = \frac{1}{3}K$ will be a rational point. It is easy to verify that the following quantities are rational: $\mathrm{sn}^2\beta$, $\sqrt{\alpha}\,\mathrm{sn}\beta\,\mathrm{cn}\beta\,\mathrm{dn}\beta$, $\mathrm{cn}\,2\beta$, $\mathrm{dn}\,2\beta$, $\sqrt{\alpha}\,\mathrm{sn}\,2\beta$, $\mathrm{sn}^2 2\beta$. Hence

$$1 = \mathrm{sn}(2\beta + \beta) = \frac{\mathrm{sn}\,2\beta\,\mathrm{cn}\beta\,\mathrm{dn}\beta + \mathrm{sn}\beta\,\mathrm{cn}\,2\beta\,\mathrm{dn}\,2\beta}{1 - k^2\mathrm{sn}^2 2\beta\,\mathrm{sn}^2\beta}.$$

Now the denominator is rational, but the numerator is not unless $\alpha = 1$, which is contrary to the present hypothesis. Hence β is not a rational point. Then 2β can not be the argument of a rational point since β, 2β, and $3\beta = K$ are collinear and K is the argument of $A_3(1, 1, 0)$.

13. **Recapitulation.** (*a*) Every cubic equation of genus one in three homogeneous variables having rational coefficients, rational anharmonic ratio, and known to have one rational solution may by a proper choice of a coördinate triangle be reduced to the form

$$xz^2 - \alpha y(y - x)(y - k^2 x) = 0, \tag{9}$$

where k^2 is a positive proper fraction and α a positive integer not containing a square factor.

(*b*) On the cubic C, the graph of (9), there will always be four rational points,

$$A_0(0, 0, 1), \quad A_1(1, 0, 0), \quad A_2(1, k^2, 0), \quad A_3(1, 1, 0),$$

with elliptic arguments

$$0, \quad iK', \quad K+iK', \quad K.$$

This is a complete four-group with rank two since two of A_1, A_2, and A_3 must be given before the remaining two can be constructed. It is made up of three complete two-groups, A_0 and A_i $(i = 1, 2, 3)$, each of rank one.

(*c*) If $\alpha = 1$, k^2 is expressible as in (14_1) or (14_2) with $1-k^2$ equal to a positive square, there will be on C four additional rational points, B_i $(i = 1, 2, 3, 4)$, each having A_3 for its tangential and lying by twos on lines through A_0, by twos on lines through A_1, and by twos on lines through A_2. The rank of this eight-group is two. The elliptic arguments of the points B_i will be

$$\tfrac{1}{2}K, \quad -\tfrac{1}{2}K, \quad \tfrac{1}{2}K+iK', \quad -\tfrac{1}{2}K+iK'.$$

Their rational coördinates are given by (16). All the points on the odd branch of the curve are expressible in terms of the real (primitive) period $\omega = 2K$, while points on the even branch will have arguments $\lambda\omega+\frac{1}{2}\omega'$, $\omega' = 2iK'$ (λ real).

(*d*) If k^2 is expressible in terms of α and of the arbitrary rational parameters s and c, in one of the forms

$$\frac{(\alpha+s^2)^2-c^2}{4\alpha s^2}, \qquad \frac{(\alpha-c)s^2+c^2}{\alpha c}, \qquad \frac{2(\alpha-s^2)}{\alpha}$$

with not simultaneously $\alpha = 1$ and $(1-k^2)$ a square, there will be on C the eight rational points already listed and in addition an infinity of rational points obtainable from these by the fundamental construction.

THE UNIVERSITY OF CHICAGO,
CHICAGO, ILL.