Rational points on cubic surfaces*.

By L. J. MORDELL in Cambridge (England).

Let a cubic surface be defined by the equation

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

where f is an irreducible polynomial with rational coefficients, or by

$$g(x, y, z, w) = 0$$

in homogeneous coordinates, where g is an irreducible homogeneous cubic polynomial with rational coefficients. There is no loss in generality in supposing that all the coefficients are integers.

The question of the rational points on the cubic surface, i. e. the solution of the equation $f(x, y, z) = 0$ in rational numbers, or of $g(x, y, z, w) = 0$ in integers, had been dormant for many years, but recently important results have been found which have added greatly to our knowledge of the subject.

Special cases arise when the equation depends essentially upon two variables, e. g. when the surface is a cone or a cylinder. The problem then becomes that of finding the rational points on a cubic curve, say $f(x, y) = 0$, where f has rational coefficients, a problem in which mathematicians have been interested for many centuries. Two types of cubic curves exist. In one the curve has a double point, O, whose coordinates are easily seen to be rational. Any line through O with rational slope, say t, will meet the cubic in only one other point, say P. Its coordinates will be determined by an equation of the first degree and so will be rational functions of a rational parameter t. Conversely every rational point on the cubic is so expressible.

When the curve has no double point, no method is known of finding a rational point on the general curve despite the efforts of mathematicians for many, many, years. But if a tangent is drawn to the curve at a known rational point, say P_1, it will in general meet the curve at another point P_{11} whose coordinates are rational since they are determined by an equation of the first degree. So the tangent at P_{11} will lead to another point $P_{11, 11}$ and we may in general find an infinity of rational points in this way. So if we

---

* Lecture held in the Mathematical Institute of the University Debrecen, December 14, 1948.

know another rational point say P_2, the chord or line joining P_1, P_2 will meet the curve in another rational point, say P_{12}, in general different from P_1 and P_2. Hence if we know any set $P_1, P_2, \ldots, P_r$ of rational points, we may in general expect to find an infinity of rational points by carrying out the tangent and chord process, adding the points thus found to the set and continuing the process. About 25 years ago, I proved that all the rational points on the curve could be found from a finite number by the chord and tangent process, and so a finite basis existed from which all rational solutions can be found. We cannot, however, at present find the basis for the general curve, though this can be done for special cases. We suppose then hereafter, that the surface is not a cone or cylinder.

Several results for the rational points on cubic surfaces have been known for two centuries. Thus the trivial case when the surface has a rational double point, typified by

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

has all its rational solutions given in terms of two rational parameters p, q on putting $x = pz$, $y = qz$.

Then about 1756, EULER solved parametrically $x^3 + y^3 = z^3 + w^3$, or say in non-homogeneous coordinates $x^3 + y^3 + z^3 = 1$. The solution is obvious from geometric considerations. The two straight lines A, $x = \varrho$, $y + \varrho z = 0$ and B, $x = \varrho^2$, $y + \varrho^2 z = 0$, where ϱ is a complex cube root of unity, lie entirely on the surface. If we take any points Q, R conjugate in the field $K(\varrho)$ on A, B respectively, the line QR meets the surface in another point P which is rational since it is determined by an equation of the first degree. The solution involves two parameters since Q and R depend upon two rational parameters. Conversely since a line can be drawn through P to meet the lines A, B, all the solutions are given in this way. The solution is given by

$$\frac{y + \varrho z}{x - \varrho} = a + b\varrho, \quad \frac{y + \varrho^2 z}{x - \varrho^2} = a + b\varrho^2,$$

and so

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

where a, b are rational parameters.

Next there is an idea of KRAFT, LAGRANGE and EULER about 1770 for solving equations by using irrational numbers. Thus a two parameter solution of $y^2 - ax^2 = z^3$ is given by taking

$$y + x\sqrt{a} = (p + q\sqrt{a})^3, \ z = p^2 - aq^2,$$

where p, q are any rational numbers. But all the solutions are not in general given in this way.

More important is the use of cubic irrationalities.

Let ϑ, φ, ψ be roots of a cubic equation with rational coefficients. Then LAGRANGE solved the homogeneous equation

$$\prod_{\vartheta,\,\varphi,\,\psi} (x+\vartheta y+\vartheta^2 z) = w^3$$

by writing

$$x+\vartheta y+\vartheta^2 z = (p+q\vartheta+r\vartheta^2)^3,$$
$$w = \prod_{\vartheta,\,\varphi,\,\psi} (p+q\vartheta+r\vartheta^2),$$

where p, q, r are rational parameters. Again, this is not the general solution.

Suppose now that a rational point P is known on the surface $f(x, y, z)=0$. The tangent plane at P meets the surface in general in an irreducible plane cubic curve with a double point at P, and so we can find at once an infinity of rational points depending on a rational parameter. This result was given essentially by LIBRI in 1820, but was probably known before that time. It was shown by B. SEGRE about 10 years ago that the exceptional case when the curve of intersection of the tangent plane broke up into three straight lines was of particular interest and of great importance in the further development.

The solution of the equations given so far have been more or less obvious. In 1826, however, RYLEY found a parametric solution of the equation

$$x^3+y^3+z^3=n$$

which is certainly not obvious, by an ingenious method whose significance seemed very obscure until fairly recently. This was until recently, practically the last essentially new result found on the rational points of cubic surfaces for more than a century. In 1930, RICHMOND found another solution of RYLEY's equation by seeking those in which x, y, z were proportional to cubic polynomials in a parameter t. The success of RICHMOND's method depended on the existence of three rational solutions of $x^3+y^3+z^3=0$, namely the inflexions $(1, -1, 0)$ etc.

But it was only ten years ago, that I solved a new equation, the first one since RYLEY's time. This was

$$(x+y+z)^3-dxyz=m, \qquad d\neq 0,$$

which includes RYLEY's $X^3+Y^3+Z^3=n$ as a special case as is seen by putting

$$x=Y+Z,\ y=Z+X,\ Z=X+Y,\ d=24,\ m=8n.$$

I found a particular solution on taking $m=dyz^2$. Then

$$(x+y+z)^3=dyz(x+z),$$

which in homogeneous coordinates is a cubic curve with a double point at $(-1, 0, 1)$. The curve meets the general line $x+z=py$ through the double point where

$$(p+1)^3 y^3 = pdy^2z,$$

or

$$\frac{y}{z} = \frac{dp}{(p+1)^3},$$

and so

$$\frac{x}{z} = \frac{dp^2}{(p+1)^3} - 1.$$

Also from $dyz^2 = m$,

$$\frac{m}{z^3} = \frac{d^2p}{(p+1)^3}.$$

On putting $p = dmt^3$ where t is a new rational parameter, clearly x, y, z are rationally expressible in termes of t.

It was this solution which was the first of these new results. Next, SEGRE found a parametric solution of the equation

$$x^3 + y^3 + az^3 = b,$$

where a, b are given rational numbers, which had previously seemed intractable. For he showed that RICHMOND's method applied to

$$xy(x+y) + az^3 = b,$$

since $xy(x+y) + az^3 = 0$ has three rational solutions given by $z = 0$, $xy(x+y) = 0$. He then made use of the well known transformation of $xy(x+y)$ into $X^3 + Y^3$.

SEGRE made then a systematic study of the arithmetical properties of cubic surfaces. Starting from LIBRI's result, he investigated the special cases when the tangent plane at a known point P met the cubic surface in a reducible curve. He showed that every cubic surface contained either 0, 1, 3 or an infinity of rational points.

Cubic surfaces with no rational points have been known for a long time, indeed not only surfaces but also eight dimensional cubic manifolds as shown by HASSE and also by myself. Thus SEGRE noted

$$x^3 + 2y^3 = 7(z^3 + 2w^3)$$

which has no solution apart from $x = y = z = w = 0$. We may suppose $(x, y, z, w) = 1$. Then since to mod 7,

$$x^3 \equiv 0, \pm 1, \; y^3 \equiv 0, \pm 1, \; x^3 + 2y^3 \equiv 0,$$

clearly

$$x \equiv 0, \; y \equiv 0.$$

Then

$$z^3 + 2w^3 \equiv 0,$$

and so

$$z \equiv 0, \; w \equiv 0.$$

Hence x, y, z, w are all divisible by 7, contrary to hypothesis.

He showed next that if cubic surfaces with only three rational points existed, they could be reduced to a canonical form, essentially

$$z^2-(1+fx)^2=ax^3+bx^2y+cxy^2+dy^3,$$

the three rational points being $(0, 0, \pm 1)$ and the point at infinity where their join meets the surface. By considering the intersections of this surface with a suitable cubic surface and a quadric surface, he was able to assign 17 points of intersection a priori, and so determined the eighteenth point rationally as a rational function of three parameters.

I then showed that a parameter solution of the equation could be found by elementary algebra, which also applied to

$$z^2-k(1+fx)^2=ax^3+bx^2y+cxy^2+dy^3,$$

by extending the method of LAGRANGE and using both quadratic and cubic irrationalities. Thus, if ϑ, φ, ψ are the roots of

$$a\xi^3+b\xi^2+c\xi+d=0,$$

I put

$$z\pm(1+fx)\sqrt{k}=\prod_{\vartheta, \varphi, \psi}[p+q\vartheta+r\vartheta^2\pm\sqrt{k}(u+v\vartheta+w\vartheta^2)]$$

where p, q, r, u, v, w are new unknowns. On writing down the condition that $(p+q\vartheta+r\vartheta^2)^2-k(u+v\vartheta+w\vartheta^2)^2$ could be written in the form $X-Y\vartheta$, it was possible to find special solutions for p, q, r, u, v, w.

SEGRE's result meant that every cubic surface had only 0 or 1 or an infinity of rational points. He showed that if there was only one rational point, the surface could be reduced to the canonical form

$$z^2=f(x, y),$$

where f is a cubic polynomial in x, y with rational coefficients.

It is easily proved that every cubic with only a finite number of rational points can be reduced to this form. The existence of any solution x_0, y_0, z_0, w_0 of the equation $g(X, Y, Z, W)=0$ leads by a substitution

$$X=x_0z+x,\ Y=y_0z+y,\ Z=z_0z,\quad W=w_0z+w$$

to an equation of the form

$$z^2L_1+zL_2+L_3=0,$$

where L_1, L_2, L_3 are homogeneous polynomials of the first, second and third degrees in x, y, w. Here L_1, L_2 are not both identically zero as then the surface would be a cone or cylinder. We may suppose L_1 is not identically zero, since there would then be an infinity of values of z given by taking arbitrary values of x, y, w for which $L_2 \neq 0$. By an appropriate linear substitution we may write $L_1=w$. We will have now an infinity of rational solutions on taking $w=0$ provided this does not imply $L_2=0$, i. e. that L_2 is divisible by w. But on putting $z - L_2/2w$ for z, the equation takes the form

$$\left(\frac{z}{w}\right)^2 = f\left(\frac{x}{w}, \frac{y}{w}\right)$$

as required.

SEGRE was able to apply my method to the equation $z^2 = f(x, y)$ and to find a parametric solution. He thus showed that every cubic surface had only none or an infinity of rational points.

Another solution of $z^2 = f(x, y)$ was found shortly after by R. F. WHITEHEAD and is so elementary that it is most suprising that it remained unknown for two centuries, and that so great a master of algebraic manipulation as EULER should have missed it.

Let us write the equation as

$$z^2 = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j$$

We may suppose without loss of generality that $a \neq 0$, and then that $a = 1$ on writing x/a for x and z/a for z.

We put $x = y^2 + ty$, where t is a rational parameter. Then

$$z^2 = y^6 + Ay^5 + By^4 + Cy^3 + Dy^2 + Ey + F,$$

say. We now put

$$z = y^3 + Py^2 + Qy + R$$

giving a quadratic equation for y whose coefficients are rational functions of t if we select P, Q, R as appropriate rational functions of t, e. g.

$$2P = A,\ 2Q + P^2 = B \text{ etc.}$$

Solving we have $y = \beta_1 \pm \beta_2 \sqrt{\Delta}$, where β_1, β_2, Δ are rational functions of t with rational coefficicnts. On substituting we find $x = \alpha_1 \pm \alpha_2 \sqrt{\Delta}$, $z = \gamma_1 \pm \gamma_2 \sqrt{\Delta}$, where the α and γ are also rational functions of t.

Now the straight line

$$\frac{x - \alpha_1}{\alpha_2} = \frac{y - \beta_1}{\beta_2} = \frac{z - \gamma_1}{\gamma_2} = r$$

meets the cubic surface in three points. Two are determined by $r^2 - \Delta = 0$, and so the third point is determined by a linear equation in r and is a rational function of the rational parameter t.

At present, necessary and sufficient conditions for the existence of one rational solution and so of an infinity are not known. I might conclude by suggesting the

Conjecture: *The equation $f(x, y, z, w) = 0$ where f is a homogeneous cubic polynomial with integer coefficients has rational solutions other than $x = y = z = w = 0$ if and only if the congruence $f(x, y, z, w) \equiv 0 \pmod{m}$ has solutions for all integers m in which x, y, z, w are not all divisible by m.*

(Received January 2, 1949.)