ARITHMETIC UPON AN ALGEBRAIC SURFACE[1]

B. SEGRE

The title of my lecture is, I am afraid, probably misleading and certainly too ambitious. For, on the one hand, the connection between arithmetic and geometry suggested by it is not the modern development in divisors theory, but an application of algebraic geometry for arithmetical purposes. On the other hand, I shall confine the subject of this lecture to cubic surfaces in ordinary space, considered in the rational domain, so that a proper title would be for instance *The geometry of ternary cubic Diophantine equations.*[2] I prefer, however, the more ambitious and inaccurate one, as suggesting the possibility of similar investigations for other surfaces, possibly considered in more general arithmetical fields.

The short time at my disposal does not allow me to dwell on such extensions. I mention only that I have already completed an extensive arithmetical research on quartic surfaces; and that the whole subject—arithmetic upon an algebraic surface—seems to me to be so wide in scope, that I can envisage the possibility of further important developments.

Let us consider an ordinary space, where coordinates (x, y, z) are introduced and points at infinity are defined in the usual way. I call *rational* an algebraic surface, or curve, or point set of this space when it can be represented by one or more algebraic equations with rational coefficients,

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

say. Moreover, I call *rational* any such equation, and also any polynomial such as $F(x, y, z)$.

The problem of finding the rational solutions in x, y, z of equation (1) can then be stated as that of determining the *rational points lying*

Received by the editors June 14, 1944.

[1] A lecture given at the London Mathematical Society, on December 16, 1943.

[2] On this subject cf. B. Segre, *A note on arithmetical properties of cubic surfaces*, J. London Math. Soc. vol. 18 (1943) p. 24; *On a parametric solution of the equation* $x^3+y^3+az^3=b$, *and on ternary forms representing every rational number*, ibid. p. 31; *On ternary nonhomogeneous cubic equations with more than one rational solution*, ibid. p. 88; *A parametric solution of the indeterminate cubic equation* $z^2=f(x, y)$, ibid. p. 226; *A complete parametric solution of certain homogeneous Diophantine equations, of degree n in* $n+1$ *variables*, ibid. vol. 19 (1944) p. 46. Another paper of mine, *On arithmetical properties of singular cubic surfaces*, will appear shortly in the same journal.

The present lecture sums up rather sketchily my previous results, to which it adds a few more, as for example the geometric construction of p. 156. Full details, together with further results, will be found in a forthcoming extensive and systematic work.

on the rational surface F, represented by (1). Moreover, a parametric solution

$$(2) \qquad x = \theta_1(\lambda)/\theta_4(\lambda), \quad y = \theta_2(\lambda)/\theta_4(\lambda), \quad z = \theta_3(\lambda)/\theta_4(\lambda)$$

of (1), where the θ's are relatively prime rational polynomials in λ, gives a *rational unicursal curve lying on F*. Likewise, a two-parameter solution

$$(3) \quad x = \theta_1(\lambda, \mu)/\theta_4(\lambda, \mu), \quad y = \theta_2(\lambda, \mu)/\theta_4(\lambda, \mu), \quad z = \theta_3(\lambda, \mu)/\theta_4(\lambda, \mu)$$

of (1), where the θ's are now relatively prime rational polynomials in λ and μ, gives a *rational representation of F upon a plane* α, on which (λ, μ) are coordinates of a variable point. The *degree* of a parametric solution (2) or (3) is defined as the greatest of the degrees of the polynomials θ in (2) or (3) respectively.

When the equations (3) induce a (1, 1)-correspondence between F and α, *all* the rational solutions of (1) are given by (3) either for rational values of the parameters λ, μ, or as limits, when the parameters tend to certain sets of rational values. Hence I shall then say that (3) is a *complete* two-parameter solution of (1).

From now on, I suppose F to be a rational cubic surface, represented by the equation (1). This can be written in the form

$$(4) \qquad \phi_0 + \phi_1(x, y, z) + \phi_2(x, y, z) + \phi_3(x, y, z) = 0,$$

where ϕ_0 is a rational number and ϕ_1, ϕ_2, ϕ_3 are homogeneous rational polynomials in x, y, z, of degrees 1, 2, 3 respectively, the two first of which may possibly vanish identically. F is said to be *singular*, if there are some points $P(x, y, z)$ (not necessarily rational, and possibly at infinity) which satisfy the equations (1) and

$$(5) \qquad \partial F/\partial x = \partial F/\partial y = \partial F/\partial z = 0.$$

Such a point P is called a *double point* of F if some of the partial derivatives of the second order of F do not vanish at P; otherwise P is called a *triple point* of F. A point $P(x, y, z)$ lying on F, that is, which satisfies (1), is called a *simple point* of F if it does not satisfy (5).

I now investigate the Diophantine equation (1) or (4), on supposing that F is irreducible and that a particular rational solution (x_0, y_0, z_0) is known. I shall show that, apart from a single trivial exception, *it is then possible to deduce an infinity of rational solutions.* By choice of the rational coordinates (x, y, z), the rational point $P(x_0, y_0, z_0)$ can be taken at the origin, so that, from (4), $\phi_0 = 0$. I distinguish three cases, according as P is a triple point, or a double point, or a simple point of F.

If P is a *triple point* of F, the equation (4) is

$$\phi_3(x, y, z) = 0,$$

and can therefore be written in the form

$$\phi_3(X, Y, 1) = 0,$$

on putting $X=x/z, Y=y/z$. The problem of finding the rational points of F is now that of determining the rational points of a plane cubic curve, and lies outside the scope of the present lecture. Hence I suppose that F has no rational triple points, and then it is easily seen that F has no irrational triple point, so that its only singular points (if any) are double points.

If the origin P is a *double point* of F, the equation (4) becomes

$$\phi_2(x, y, z) + \phi_3(x, y, z) = 0, \tag{6}$$

where ϕ_2 and ϕ_3 are two relatively prime polynomials, neither of which vanishes identically. There is now a (1,1)-correspondence between the rational points Q of F and the rational lines PQ containing P. This gives the following *complete* two-parameter solution of (6), of degree three:

$$x = -\lambda\phi_2(\lambda, \mu, 1)/\phi_3(\lambda, \mu, 1), \qquad y = -\mu\phi_2(\lambda, \mu, 1)/\phi_3(\lambda, \mu, 1),$$
$$z = -\phi_2(\lambda, \mu, 1)/\phi_3(\lambda, \mu, 1).$$

If P is a *simple point* of F, then in (4) we have $\phi_0=0$ but $\phi_1(x, y, z)$ does not vanish identically, and the equation $\phi_1(x, y, z)=0$ represents the plane π touching F at P. On taking this plane as xy-plane, the equation of F becomes of the form

$$z + \phi_2(x, y, z) + \phi_3(x, y, z) = 0, \tag{7}$$

and I further distinguish two cases, according as $\phi_2(x, y, 0)$ vanishes identically or not.

When $\phi_2(x, y, 0)\neq 0$, there is a (1,1)-correspondence between the rational points Q of F lying on π and the rational lines PQ of π containing P. Such ∞^1 points Q are said to be obtained by means of the *tangent plane process* applied to F and P, and are all given by the following one-parameter solution of (7):

$$x = -\lambda\phi_2(\lambda, 1, 0)/\phi_3(\lambda, 1, 0), \quad y = -\phi_2(\lambda, 1, 0)/\phi_3(\lambda, 1, 0), \quad z = 0.$$

When $\phi_2(x, y, 0)=0$ the tangent plane process cannot be applied, and the equation (7) has the form

$$z[1 + \psi_1(x, y, z)] + \phi_3(x, y, z) = 0,$$

where ψ_1 is a rational linear form in x, y, z. Hence, on putting

$$X = x/z, \qquad Y = y/z, \qquad Z = [1 + 2^{-1}\psi_1(x, y, z)]/z,$$

this equation reduces to the form

$$Z^2 = f(X, Y), \tag{8}$$

where f is a rational cubic polynomial in X, Y, which cannot be written as a polynomial in a single linear function of X and Y.

I have recently *solved parametrically the general equation* (8), by first reducing it to a convenient canonical form, and then using a method which has been already employed by Professor Mordell in a particular case. Here I solve the equation in another particular case, which is perhaps the simplest one in which the method can be applied. I add that I have previously solved parametrically some cubic Diophantine equations included in (8), by considerations of algebraic geometry. Professor Mordell then devised his purely algebraic method, giving an independent proof and also an extension of these results of mine. I give now also a new algebraic-geometric process for solving parametrically the equation of any rational cubic surface of which a rational simple point is known. This process can be applied to (8) in particular, and has the advantage of making intuitive the solvability of this equation.

I solve first the following particular case of (8):

$$z^2 - ry^2 = x^3 + px + q, \tag{9}$$

where p, q, r are rational and $r \neq 0$. For this purpose, I remark that, on denoting by θ, ϕ, ψ the three roots of the cubic equation $x^3+px+q=0$ and putting

$$\begin{aligned} z + r^{1/2}y &= \prod_{\theta,\phi,\psi} [\xi + \lambda\theta^2 + r^{1/2}(\eta + \mu\theta)], \\ z - r^{1/2}y &= \prod_{\theta,\phi,\psi} [\xi + \lambda\theta^2 - r^{1/2}(\eta + \mu\theta)], \end{aligned} \tag{10}$$

the equation (9) is satisfied if

$$x - \theta = (\xi + \lambda\theta^2)^2 - r(\eta + \mu\theta)^2 \tag{11}$$

holds, together with two other similar relations in ϕ and ψ. Writing, in (11), $-p\theta^2-q\theta$ for θ^4 and comparing coefficients of θ^0, θ^1, θ^2, we obtain

$$\begin{aligned} x &= \xi^2 - r\eta^2, \\ 1 &= q\lambda^2 + 2r\mu\eta, \\ 0 &= 2\lambda\xi - p\lambda^2 - r\mu^2. \end{aligned} \tag{12}$$

The last two equations give

$$\xi = (p\lambda^2 + r\mu^2)/2\lambda, \qquad \eta = (1 - q\lambda^2)/2r\mu.$$

Hence, on substituting these expressions for ξ, η in (12), and in the two relations obtained by subtracting and adding the equations (10) together, we deduce x, y, z as rational functions of λ, μ, with rational coefficients, satisfying (9).

I consider next a rational cubic surface F, of which a rational simple point P is known, and give the following *geometric construction* leading always to *an infinity of rational points of F.*

A rational line r passing through P meets F again in a rational pair of points, H, K say. This means that H, K are either rational or quadratic conjugate; and we can suppose, by choice of r, that H, K, and P are distinct. I fix then another rational line s in a general position, and consider the twisted cubic curve, Γ say, uniquely defined by the conditions of osculating at H, K the sections of F with the planes Hs, Ks respectively. It is easily seen that Γ is rational and irreducible and does not lie on F. Hence Γ and F meet at $3\cdot 3=9$ points, of which three are absorbed by H and three are absorbed by K, so that the remaining intersections constitute a rational triplet, M, N, O say. These three points are noncollinear and lie in a plane which does not contain P.

Denoting by π the (obviously rational) tangent plane of F at P, I finally consider the quadrics touching π at P and containing M, N, O. These quadrics constitute a homaloidal system. It can be proved by means of the Cremonian transformation defined by them that it is possible to choose (in an infinity of ways) two such quadrics, so that their intersection is an irreducible rational quartic curve, Δ say, touching F at M, N, and O. Δ does not lie on F, and so meets F at $3\cdot 4=12$ points, of which four are absorbed by P and two are absorbed by each of the points M, N, O. The remaining intersections are

$$12 - 4 - 2\cdot 3 = 2$$

in number, and form a rational pair, S, T say. Clearly the line ST is rational and does not lie on F; moreover ST does not contain P, since Δ has no trisecants. Hence ST meets F again at a point which is distinct from P and uniquely defined, and therefore rational. This rational point assumes an infinity of positions on F, on varying the lines r, s and the quartic Δ considered above.

It is easily seen that the irreducible rational cubic surfaces F which are *singular*, but not of the types already investigated, are of the following three kinds.

(i) F has four nonrational and noncoplanar double points.

(ii) F has three nonrational and noncollinear double points.

(iii) F has two nonrational double points.

I state now the following results concerning the corresponding Diophantine equations.

In case (i), *it is possible to obtain a complete rational two-parameter solution of the 3rd degree.*

In case (ii), *there may be no rational solutions. When any particular rational solution is known, it is possible to deduce a complete rational two-parameter solution of the 6th degree. No complete two-parameter solution of degree less than six exists, except when F satisfies certain arithmetical conditions, in which case F has a complete rational two-parameter solution of the 3rd degree.*

In case (iii), *F can always be solved parametrically, but in general there are no complete two-parameter solutions.*

In case (i), there is an infinity of rational twisted cubic curves containing the four double points of F, say A, B, C, D. In general one of these cubics is irreducible and does not lie on F, and so it has $3\cdot 3=9$ intersections with F, of which $2\cdot 4=8$ are absorbed by A, B, C, D. Hence the remaining intersection is rational. It is possible to construct in this way *all* the rational points of F. A *complete* two-parameter solution of the 3rd degree can be obtained, on transforming F into a rational plane by means of the homaloidal system formed by the ∞^3 cubic surfaces having four double points at A, B, C, D. Similar geometric arguments can be applied in case (ii).

These indications may suffice, and I add only the following applications concerning two particular cubic Diophantine equations of types (i) and (ii) respectively.

First put

$$\Phi = (ky^2 - 2kxz + t^2)^2 - k(x^2 + kz^2 - 2yt)^2,$$
$$\Psi = (k\mu^2 - 2k\lambda\nu + \omega^2)^2 - k(\lambda^2 + k\nu^2 - 2\mu\omega)^2,$$

where k denotes any nonzero rational number, and consider the cubic homogeneous Diophantine equation in x, y, z, t:

$$a\partial\Phi/\partial x + b\partial\Phi/\partial y + c\partial\Phi/\partial z + d\partial\Phi/\partial t = 0, \tag{13}$$

where a, b, c, d are any four rational numbers not all zero. A *complete* two-parameter solution of (13) is then

$$x:y:z:t = \frac{\partial\Psi}{\partial\nu}:\frac{\partial\Psi}{\partial\mu}:\frac{\partial\Psi}{\partial\lambda}:k\frac{\partial\Psi}{\partial\omega}, \tag{14}$$

where the parameters are subject to the linear equation

$$k(c\lambda + b\mu + a\nu) + d\omega = 0. \tag{15}$$

More precisely, *all* the rational solutions of (13) are given by (14) for rational values of $\lambda:\mu:\nu:\omega$ subject to (15), if k is not the square of a rational number. If $k=\rho^2$, with ρ rational, the equation (13) has the additional solutions

$$x + \rho z = t + \rho y = 0 \quad \text{and} \quad x - \rho z = t - \rho y = 0.$$

Secondly consider the rational cubic equation

$$a\theta^3 + b\theta^2 + c\theta + d = 0 \qquad (a \neq 0), \tag{16}$$

and suppose that it has three nonrational (and therefore distinct) roots θ, ϕ, ψ. Hence (16) has a nonzero discriminant

$$D = -27a^2d^2 - 4ac^3 + 18abcd - 4db^3 + b^2c^2.$$

It is easily seen that the rational cubic equation

$$\prod_{\theta,\phi,\psi} (x + y\theta + z\theta^2) = 1 \tag{17}$$

is of type (ii). This equation has been solved parametrically by Lagrange and Euler by taking

$$x + y\theta + z\theta^2 = (\lambda + \mu\theta + \nu\theta^2)^3 / \prod_{\theta,\phi,\psi} (\lambda + \mu\theta + \nu\theta^2) \tag{18}$$

and so on, where λ, μ, ν are parameters of which only the ratios are significant. The rational two-parameter solution of (17) given by (18) is of the 3rd degree, and, in agreement with a previously quoted result, is *noncomplete*. With the method indicated, however, it is possible, from the particular solution

$$x = 1, \qquad y = 0, \qquad z = 0$$

of (17), to deduce a *complete rational two-parameter solution of the 6th degree*. Moreover, it can be proved that *the equation* (17) *has a complete rational two-parameter solution of degree less than six if and only if the discriminant D of* (16) *is the square of a rational number*. When this condition is satisfied, (17) has in fact the *complete rational two-parameter solution of the 3rd degree* defined by the equation

$$x + y\theta + z\theta^2 = (\lambda + \mu\phi + \nu\phi^2)(\lambda + \mu\psi + \nu\psi^2)^2 / \prod_{\theta,\phi,\psi} (\lambda + \mu\theta + \nu\theta^2)$$

and by those obtained from it on permuting θ, ϕ, ψ cyclically.

I consider now the cubic surfaces which are *nonsingular*.[3] It is well

[3] For a new approach to these surfaces, cf. B. Segre, *The non-singular cubic surfaces*, Oxford, 1942.

known that any such surface F contains 27 lines, each of which may of course be rational or not. I first remark that *F may contain no rational points*, as it is shown by the examples

$$x^3 + 2y^3 + 4z^3 = 9 \quad \text{and} \quad x^3 + 2y^3 + 7z^3 = 14,$$

which can be easily generalized.

The determination of necessary and sufficient conditions for the existence of rational points on F is an important and difficult question. I have not succeeded in solving this problem, but the considera- of certain arithmetical properties for the lines of F leads to some sufficient conditions.

It must be noticed that *F cannot contain one rational point without consequently having an infinity of rational points.* For, since F is nonsingular, a *rational parametric solution* can always be deduced from a single rational solution, as said before (p. 156). The number of parameters involved is not essential, and can be made arbitrarily large by a repeated application of the tangent plane process. In particular, it follows easily that:

A nonsingular cubic surface F can be rationally represented upon a plane α if and only if F contains a rational point.

Such a representation does not give in general a (1, 1)-*correspondence* between F and α. In fact, for the existence of a representation having this property, further conditions are required from F. I have studied these conditions, as well as those for the existence on F of *nontrivial rational curves*, that is, of rational curves which are not the complete intersection of F with another rational surface. The results are unexpectedly simple, but I have no time now to dwell on them. I confine myself to pointing out the remarkable fact that these arithmetical conditions affect the 27 lines of F only.

The 27 lines of the cubic surface

$$ax^3 + by^3 + cz^3 = 1 \qquad (abc \neq 0) \tag{19}$$

can be obtained easily, and the general theory leads now to particularly simple results. On altering, in (19), x, y, z by arbitrary nonzero rational factors, and permuting arbitrarily x, y, z, we obtain an infinity of equations of the same type as (19), any two of which will be called *equivalent.*

I first consider the equations

$$ax^3 + acy^3 + cz^3 = 1 \qquad (ac \neq 0), \tag{20}$$

$$a(x^3 + y^3) + z^3 = 1 \qquad (a \neq 0), \tag{21}$$

$$x^3 + y^3 + z^3 = 1, \tag{22}$$

which obviously are successive particularizations of (19). I can then state the result:

A cubic surface (19) *contains some nontrivial rational curves, if and only if* (19) *is equivalent to an equation of the form* (20). *This condition is also necessary, but not sufficient, for* (19) *to have a complete rational two-parameter solution. An equation* (19) *has a rational two-parameter solution of degree three or four, possibly noncomplete, if and only if* (19) *is equivalent to an equation of the form* (22) *or* (21) *respectively.*

Such parametric solutions of (22) and (21) have already been obtained by Euler and Hermite respectively, and these are both *complete.* I add that there are *equations* (20) *having no rational solutions,* as for example, the one obtained from (20) for $a=1/2$, $c=1/7$. *When a single rational solution of* (20) *is known, it is possible to determine a complete rational two-parameter solution of* (20), *of degree six.*

I consider next the following particularizations of (19):

$$x^3 + y^3 + kz^3 + k = 0, \tag{23}$$

$$x^3 + y^3 + kz^3 + 2 = 0, \tag{24}$$

$$x^3 + y^3 + 2z^3 + 2 = 0, \tag{25}$$

where k is a nonzero rational number which is not twice the cube of a rational number, and state the following theorem.

The equation (19) *has solutions with* x, y, z *rational polynomials in a parameter* λ, *of degree four or less, if and only if* (19) *is equivalent to one of the equations* (23), (24), (25). *By a proper choice of* λ, *the solutions are as follows. The equation* (23) *has only the solutions*

$$x = \lambda, \qquad y = -\lambda, \qquad z = -1$$

and

$$x = -(9/k)\lambda^4 + 3\lambda, \qquad y = (9/k)\lambda^4, \qquad z = (9/k)\lambda^3 - 1.$$

The equation (24) *has only the solution*

$$x = (6/k)\lambda^3 - 1, \qquad y = -(6/k)\lambda^3 - 1, \qquad z = (6/k)\lambda^2.$$

The equation (25), *in addition to the three solutions given for* $k=2$ *by the previous expressions, has only the further solutions*

$$x=4\lambda^2-6\lambda+1, \quad y=4\lambda^2-2\lambda-1, \quad z=-4\lambda^2+4\lambda-1 \qquad \textit{and}$$

$$x=(2/27)(4\lambda^4-4\lambda^3-6\lambda^2+17\lambda-2),$$
$$y=(4/27)(2\lambda^4-8\lambda^3+6\lambda^2+4\lambda-13),$$
$$z=(1/27)(-8\lambda^4+20\lambda^3-24\lambda^2-16\lambda+37).$$

The particular result following from this theorem on supposing

$a=b=c$ in (19) has previously been obtained by Professor Mordell, in an entirely different way.

In conclusion, I regret I have had to dwell more on my results than on my methods. The latter are purely algebraic-geometric in character and, as I said at the beginning, can be extended and employed in other directions.

It may be noticed that my work does for cubic surfaces what Poincaré did for plane cubic curves more than 40 years ago. In my work, however, the use of geometry is more essential and far-reaching, since there are several properties of cubic surfaces which are arithmetically significant, and have no counterpart for plane cubic curves. For instance, the general cubic surface F is homaloidal, that is, F can be related in the complex domain to a plane by a $(1,1)$ algebraic correspondence. A similar result does not hold for the general plane cubic curve, since this is not unicursal, but elliptic. Another important property having no analogue for plane cubic curves is that F contains 27 lines, and that every algebraic curve lying on F can be constructed as partial intersection of F with another algebraic surface, the residual intersection being a set of lines of F taken with proper multiplicities.

It ought to be mentioned that a few interesting, but isolated and comparatively elementary, examples of application of geometric ideas in the study of cubic ternary Diophantine equations have been given by Libri, Euler, Hermite and, in recent times, by H. W. Richmond.

I am glad to have the opportunity of acknowledging that I owe the first stimulus for my research to Professor Mordell, who, a little more than a year ago, pointed out to me the geometric results of the authors just named, as well as his own arithmetical results on sums of three cubes.

THE UNIVERSITY,
MANCHESTER, ENGLAND