SOME RELATIONS BETWEEN THE THEORY OF NUMBERS

AND OTHER BRANCHES OF MATHEMATICS

By Leonard Eugene DICKSON

(Chicago).

I have chosen the subject of my address before the Congress from the field of the theory of numbers, the literature of which I had been examining minutely in the preparation and publication of the first two volumes of my *History of the Theory of Numbers* [1]. I shall approach a few typical problems of the theory of numbers through the medium of other branches of mathematics.

Accordingly I shall first apply geometrical methods to find all the rational solutions of certain homogeneous Diophantine equations. I do not consider equations of the second degree since all their rational solutions can be found at once when one solution is known; in fact, we can evidently represent parametrically all the points of a quadric surface by making use of the secant lines through a chosen point on it.

My second topic relates to the more difficult question of finding one or more formulas which give all the integral solutions when the parameters take only integral values. While seeking interesting material which would illustrate this topic, I was led to the discovery of a very simple general method of finding explicit formulas which give all the integral solutions of homogeneous quadratic equations in several variables. For equations in four variables, the method makes use of some simple properties of integral algebraic numbers; while for equations in six variables, use is made of properties of integral quaternious. Since it is the purpose of this address to point out applications of several branches of mathematics to the theory of numbers in its elementary sense, I take this opportunity to demonstrate the fact that the theories of algebraic and hypercomplex numbers provide effective tools for the treatment of Diophantine equations.

Finally, I shall point out how invariants came to be employed quite naturally in the theory of numbers.

[1] Carnegie Institution, Washington, D. C., 1919, 1920.

I. Geometrical methods of finding all the rational solutions of certain Diophantine equations.

We shall indicate several methods of finding all the rational points on certain cubic surfaces, partly with the aim to show the intuitive character of the geometrical treatment of homogeneous Diophantine equations, but mainly with the aim to show why we should expect a variety of types of formulas each giving all the rational solutions of the equation, and also to point out that we can pass from one such formula to the others by means of birational transformations.

To have a concrete illustration, take the equation

$$(1) \qquad . \, x^2y + y^2z + z^2u + u^2x = 0,$$

which Hermite proposed as an exercise. The most evident geometrical method of solution makes use of the skew rulings (straight lines lying on the surface)

$$\mathrm{R}_1 : \quad y = u = 0; \qquad \mathrm{R}_2 : \quad x = z = 0.$$

Any straight line L which intersects both R_1 and R_2 will meet the surface in an unique third point (unless L is a ruling), whose coordinates are therefore determined rationally. The general point on R_1 is $(a, 0, b, 0)$; that on R_2 is $(0, c, 0, d)$. The general point on the line joining these points is (ma, nc, mb, nd), which is on the surface (1) if and only if

$$mn \{ m(a^2c + b^2d) + n(ad^2 + bc^2) \} = 0 .$$

From $mn = 0$, we obtain the initial points. The final factor gives the desired solution

$$(2) \qquad \begin{cases} \rho x = - a(ad^2 + bc^2), & \rho y = c(a^2c + b^2d), \\ \rho z = - b(ad^2 + bc^2), & \rho u = d(a^2c + b^2d). \end{cases}$$

In case the above final factor is identically zero, we see that $a \neq 0$ and hence may take $a = 1$, whence $c = - b^2d$, $b^5 = - 1$. The resulting real points are $(m, \, - nd, \, - m, \, nd)$, which lie on the ruling

$$\mathrm{R}_3 : \qquad z = - x, \quad u = - y.$$

Hence *all real solutions, except those on this ruling* R_3, *are given by formulas* (2).

Since the points of a surface depend upon the ratios of only three parameters, we may reduce by one the number of homogeneous parameters in our solution (2).

This is also evident since only the ratios $a : b$ and $c : d$ were essential in our initial points. First, let a and c be different from zero. Divide equations (2) by a^2c^2 and write

$$\frac{b}{a}=\frac{\mu}{\lambda}, \qquad \frac{d}{c}=\frac{\nu}{\lambda},$$

retaining the common denominator λ so that also our final formulas shall be homogeneous. We obtain

$$(3) \qquad \begin{cases} \sigma x = -\lambda^2(\lambda\mu+\nu^2), & \sigma y = \lambda(\lambda^3+\mu^2\nu), \\ \sigma z = -\lambda\mu(\lambda\mu+\nu^2), & \sigma u = \nu(\lambda^3+\mu^2\nu). \end{cases}$$

Next, if $a = 0$ and hence $b \neq 0$, we may take $b = 1$ in (2) and obtain the points $(0, cd, -c^2, d^2)$ on the conic $y^2 + zu = 0$, which with R_2 is the section of our surface by the plane $x = 0$. Finally, if $c = 0$, we may take $d = 1$ and obtain the points $(-a^2, 0, -ab, b^2)$ on the conic $z^2 + ux = 0$, which with R_1 is the section by $y = 0$. Hence *all the real points on the surface* (1) *are given by formulas* (3) *together with the points on the preceding conics and those on the ruling* R_3. These three classes of points are actually exceptional, not being cases of (3).

There is a second geometrical method of solving equation (1). Writing it in the determinantal form

$$\begin{vmatrix} z & -x & 0 \\ x & y & -u \\ u & z & y \end{vmatrix} = 0,$$

we see that the surface is the locus of the intersections of corresponding planes of three projective bundles of planes (each bundle being the totality of planes through a point):

$$\begin{aligned} \lambda z - \mu x \qquad &= 0, \\ \lambda x + \mu y - \nu u &= 0, \\ \lambda u + \mu z + \nu y &= 0. \end{aligned}$$

Solving these for the ratios of the coordinates, we get

$$\frac{z}{x}=\frac{\mu}{\lambda}, \qquad \frac{y}{x}=\frac{\lambda^3+\mu^2\nu}{-\lambda(\lambda\mu+\nu^2)}, \qquad \frac{u}{x}=\frac{\mu^3-\lambda^2\nu}{-\lambda(\lambda\mu+\nu^2)}.$$

Hence we have the solution

$$(4) \qquad \begin{cases} \rho x = -\lambda(\lambda\mu+\nu^2), & \rho y = \lambda^3+\mu^2\nu, \\ \rho z = -\mu(\lambda\mu+\nu^2), & \rho u = \mu^3-\lambda^2\nu, \end{cases}$$

which was published by Hermite [1] without indication of his method. The above theory is applicable to any cubic surface [2].

The algebraic equivalence of the two solutions (3) and (4) can be explained by use of a general principle. When, as here, we have two parametric representations of all the points of an unicursal surface, the two sets of parameters are connected by a birational transformation. In fact, either representation is a correspondence, which is one-to-one in general, betwen the points of the surface and the points $\lambda : \mu : \nu$ of a plane. Hence the ratios of λ, μ, ν are expressible rationally in terms of the ratios of x, y, z, u. Inserting the values of the latter in terms of the parameters λ_1, μ_1, ν_1 of the second representation, we obtain the desired birational transformation. In our case, equations (3) give

$$\frac{\mu}{\lambda}=\frac{z}{x}, \qquad \frac{\nu}{\lambda}=\frac{u}{y},$$

and two values for σ which are consistent in view of the equation (1) of the surface. Inserting the values (4) of x, y, z, u expressed in terms of λ_1, μ_1, ν_1 we get

$$\frac{\mu}{\lambda}=\frac{\mu_1}{\lambda_1}, \qquad \frac{\nu}{\lambda}=\frac{\mu_1^3-\lambda_1^2\nu_1}{\lambda_1^3+\mu_1^2\nu_1}.$$

The last equation is linear in ν_1. Solving, we get

$$\frac{\mu_1}{\lambda_1}=\frac{\mu}{\lambda}, \qquad \frac{\nu_1}{\lambda_1}=\frac{\mu^3-\lambda^2\nu}{\lambda^3+\mu^2\nu}.$$

Hence the transformation is birational and is its own inverse [3].

We can birationally transform our solutions into solutions of fifth and higher degrees in the parameters. But there exists no solution which is homogeneous and quadratic in three independent parameters, since [4] a cubic surface having this property is a ruled surface with a double line, whereas our cubic (1) has no singular point.

The first of the above methods is not limited to cubic surfaces having two skew

[1] *Nouv. Ann. Math.*, sér. 2, tome 6, 1867, p. 95. S. Realis, *ibid.*, sér. 2, t. 18, 1879, pp. 302-4, stated a special homogeneous solution of degree 4 in 2 parameters. M. Weill, *ibid.*, sér. 3, t. 4, 1885, pp. 184-8, gave an algebraic discussion requiring four cases.

[2] H. Schröter, *Jour. für Math.*, t. 62, 1863, p. 265. A. Clebsch, *ibid.*, t. 65, 1866, p. 359. L. Cremona, *ibid.*, t. 68, 1868, p. 82, and *Memorie Accad. Sc. Istituto di Bologna*, sér. 2, t. 6, t. 7 (German transl. by M. Curtze, *Allgemeinen Theorie der Oberflächen*, 1870).

[3] This may be explained by noting that, if $\lambda = 1$, the values of x, y, z are the same in (3) and (4), while the two values of u are merely the two roots of (1) regarded as a quadratic equation for u.

[4] Salmon, *Geometry of Three Dimensions*, ed. 4, 1882, p. 556, § 585.

rulings with rational coefficients, but is applicable also when the surface has two skew rulings whose equations involve a single square root. For example, the surface

$$(5) \qquad f(x, y) = f(u, z), \qquad f(x, y) \equiv Ax^3 + Bx^2y + Cxy^2 + Dy^3,$$

contains the skew rulings

$$R_4 : \; x = \omega u, \; y = \omega z; \qquad R_5 : \; x = \omega^2 u, \; y = \omega^2 z,$$

where ω is an imaginary cube root of unity. The line

$$L : \; x = ay + bz, \qquad u = cy + dz$$

meets both R_4 and R_5 if and only if $b = -c$, $d = a + c$. Now L meets (5) in the points for which $\alpha y^3 + \ldots - \beta z^3 = 0$, where

$$(6) \qquad \alpha = f(a, 1) - Ac^3, \qquad \beta = f(d, 1) + Ac^3, \qquad d = a + c.$$

But if $y = \omega z$, the equations for L give $x = \omega u$. Hence to discard the points which lie on R_4 and R_5, we remove from $\alpha y^3 + \ldots - \beta z^3$ the factor $(y - \omega z)(y - \omega^2 z)$ and obtain $\alpha y - \beta z = 0$ for the unique third point in which L meets (5). Unless $\alpha = \beta = 0$, the coordinates of this point are

$$(7) \qquad \rho y = \beta, \qquad \rho z = \alpha, \qquad \rho x = a\beta - c\alpha, \qquad \rho u = c\beta + (a + c)\alpha.$$

Finally, if the equations of a line L′ are not solvable for x and u in terms of y and z, and if L′ meets both R_4 and R_5, we find that L′ is $y = z = 0$, which meets (5) in the single real point having also $x = u = 1$ (if $A \neq 0$). *Except for this point and the points on a possible ruling of the form* L (*with* $\alpha = \beta = 0$), *all the real points on the surface* (5) *are given parametrically by formulas* (7), *in which* α *and* β *are defined by* (6).

For the case $f(x, y) = x^3 + y^3$, this method was given by Hermite [1].

The same method yields an explicit formula for all the rational solutions of

$$f(x_1, x_2, x_3) = f(y_1, y_2, y_3),$$

where f is any ternary cubic form. We have only to use the two-dimensional « ruling » $x_i = \omega y_i \; (i = 1, 2, 3)$ instead of R_4, and a line L whose equations express x_1, x_2. y_1, y_2 in terms of x_3, y_3.

[1] *Nouv. Ann. Math.*, sér. 2, t. 11, 1872, pp. 5-8; *Œuvres*, III, pp. 115-7.

The method was employed by G. Brunel [1] to find the rational solutions of

$$x_1^p + x_2^p = \begin{vmatrix} y_1 & y_2 & \cdots & y_{p-1} & 0 \\ 0 & y_1 & \cdots & y_{p-2} & y_{p-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ y_2 & y_3 & \cdots & 0 & y_1 \end{vmatrix},$$

where p is an odd prime.

There are of course unicursal surfaces other than the quadric and cubic surfaces. As noted by A Clebsch [2], we can represent parametrically (map on a plane) the points of a quartic surface having a double conic by selecting any one of the 16 ruled lines (each of which meets the conic) and drawing through any point P on the surface a line L which meets both the conic and the selected ruled line; then if L meets the plane of representation at P′, we have a one-to-one correspondence between the points P and P′. This problem can, however, be reduced to the one which we have been considering above, since Geiser [3] proved that such a quartic surface can be transformed birationally into a cubic surface. Clebsch also mapped on a plane quartic surfaces with a double line and quintic surfaces with a double skew cubic. Further references were given by Cayley [4].

II. Application of algebraic and hypercomplex numbers to the complete solution in integers of certain Diophantine equations.

We next present a new method which leads very simply to explicit formulas giving all the solutions in integers of certain quadratic equations such as

$$x_1^2 + x_2^2 + x_3^2 = x_4^2, \qquad x_1^2 + \ldots + x_5^2 = x_6^2.$$

Incidentally, we shall note the marked contrast between the problem of finding all the rational solutions and that of finding all the solutions in integers, in spite of the homogeneity of our equations. For each equation we transpose one square and express the difference of two squares as a product.

Consider therefore the equation

$$(1) \qquad x^2 + y^2 = zw.$$

[1] *Mém. Soc. Sc. Phys. Nat. Bordeaux*, sér. 3, t. II, 1886, p. 129.

[2] *Math. Annalen*, t. I, 1869, pp. 253-316.

[3] *Jour. für Math.*, t. 70, 1869, pp. 249-257.

[4] *Proc. London Math. Soc.*, t. 3, 1869-71, p. 192.

Its rational solutions are found at once. If $z \neq 0$, we may write

$$\frac{x}{z}=\frac{n}{m}, \qquad \frac{y}{z}=\frac{r}{m},$$

where m, n, r, are integers without a common factor > 1. Then

$$\frac{w}{z}=\left(\frac{x}{z}\right)^2+\left(\frac{y}{z}\right)^2=\frac{n^2+r^2}{m^2}.$$

We may take $z=\rho m^2$, where ρ is rational. Then

$$(2) \qquad x=\rho mn, \qquad y=\rho mr, \qquad z=\rho m^2, \qquad w=\rho(n^2+r^2).$$

The rational solutions of (1) with $z=0$ have $x=y=0$ and hence are given by (2) for $m=0$. While therefore (2) gives all the rational solutions of (1) when ρ is rational and m, n, r are integers without a common factor, (2) does not give all solutions in integers when ρ is restricted to integral values. In fact, if the solution $x=1, y=3, z=2, w=5$ be of the form (2), we find by dividing the values of y and z by x that $3n=r$, $2n=m$. Since n is therefore a common factor of r, m, n, we have $n=\pm 1$, whence $m=\pm 2$, $r=\pm 3$, $\rho=1/2$. Similarly, to obtain the permuted solution $x=1, y=3, z=5, w=2$, we must take $n=\pm 1$, $m=\pm 5$, $r=\pm 3$, $\rho=1/5$.

To obtain a formula which gives all the integral solutions of equation (1) for integral values of the parameters, we have only to employ the well-known fact that the norm x^2+y^2 of the product

$$(3) \qquad x+yi=(m+qi)(n+ri)$$

of two complex numbers equals the product of their norms. Thus (1) has the solution

$$(4) \qquad x=mn-rq, \qquad y=mr+nq, \qquad z=m^2+q^2, \qquad w=n^2+r^2.$$

We shall restrict attention to integral values of m, n, q, r without a common factor. The products of the resulting numbers (4) by an arbitrary rational number ρ give all the rational solutions of (1), since these products reduce to (2) when $q=0$.

We proceed to prove that we obtain all the integral solutions when we restrict the multiplier ρ to integral values. We have merely to show that, when the products of the numbers (4) by an irreducible fraction s/p are equal to integers, so that the numbers (4) are divisible by p, then the quotients are expressible in the same form (4) with new integral parameters in place of m, n, q, r. It is sufficient to prove this for the prime factors (equal or distinct) of p, since after each of them has been divided out in turn, p itself has been divided out.

Let therefore p be a prime number which divides the four numbers (4). If p divided both m and n, it would divide also q and r, in view of z and w, which is contrary to hypothesis. But if we interchange m and n, as well as q and r, we see that x and y remain unaltered, while z and w are interchanged. Hence we will be treating one of two entirely similar cases if we assume that m is not divisible by p.

We now make use of the fact that complex integers $m + qi$, where m and q are ordinary integers, obey the laws of divisibility of arithmetic. Hence, since p divides the product z of $m + qi$ and $m - qi$, without dividing either factor, we conclude that p is not a complex prime, but decomposes into

$$p = (s + ti)(s - ti), \tag{5}$$

where $s \pm ti$ are complex primes (since otherwise p would be a product of three factors and its norm p^2 would be a product of three integers each > 1). By choice of the sign of t, we may assume that $s + ti$ is that one of the prime factors $s \pm ti$ of p which divides $m + qi$, and write

$$m + qi = (s + ti)(\mathrm{M} + \mathrm{Q}i), \qquad z = m^2 + q^2 = p(\mathrm{M}^2 + \mathrm{Q}^2), \tag{6}$$

where M and Q are integers. Since x and y are divisible by p, while $m + qi$ is divisible by $s + ti$ but not by the product (5), it follows from (3) that $n + ri$ is divisible by $s - ti$:

$$n + ri = (s - ti)(\mathrm{N} + \mathrm{R}i), \qquad w = n^2 + r^2 = p(\mathrm{N}^2 + \mathrm{R}^2), \tag{7}$$

where N and R are integers. Comparing the product of (6) and (7) with (3), we have

$$x + yi = p(\xi + \eta i), \qquad \xi + \eta i \equiv (\mathrm{M} + \mathrm{Q}i)(\mathrm{N} + \mathrm{R}i).$$

Hence the integral quotients $\xi = x/p$, $\eta = y/p$, z/p, w/p, are of the form (4) with m, n, q, r replaced by the integers M, N, Q, R. Thus *all the integral solutions of $x^2 + y^2 = zw$ are obtained by multiplying an arbitrary integer into the numbers* (4) *in which m, n, q, r are integers without a common factor.* In brief, the equation is solved by the formula which expresses the fact that the norm of the product of two complex integers equals the product of their norms.

We have presented this proof in great detail partly on account of its simplicity and elegance, and partly to be able to point out the minor alterations necessary to extend the proof to a variety of important Diophantine equations.

We deduce at once all the integral solutions of

$$x_1^2 + x_2^2 + x_3^2 = x_4^2.$$

After removing the greatest common divisor of x_1, x_2, x_3, we may assume that x_1 is odd. Then x_2 and x_3 are even, since every square is of the form $4n$ or $4n+1$. We may therefore write

$$x_2 = 2x, \qquad x_3 = 2y, \qquad x_4 - x_1 = 2z, \qquad x_4 + x_1 = 2w,$$

where x, y, z, w are integers satisfying (1), and hence are equal to products of numbers (4) by an arbitrary integer.

The preceding discussion continues to hold true after we replace $x + yi$ by $x + y\theta$, where θ is a root of any one of the following eight equations:

$$\theta^2 = \pm 2, \quad \theta^2 = 3, \quad \theta^2 + \theta + k = 0 \qquad (k = \pm 1, \quad 2, \quad \pm 3),$$

since the numbers $x + y\theta$, where x and y are integers, obey the laws of divisibility of arithmetic. For the final quadratic equation, the norm of $x + y\theta$ is $x^2 - xy + ky^2$. Hence the formula which expresses the fact that the norm of a product equals the product of the norms of the two factors leads to all the integral solutions of

$$(8) \qquad x^2 - xy + ky^2 = zw.$$

We readily deduce all the integral solutions of

$$(9) \qquad x_1^2 + (4k - 1)x_2^2 + x_3^2 = x_4^2.$$

We may assume that one of x_1 and x_3 is congruent to x_2 modulo 2 and then, by permuting them if necessary, assume that $x_1 \equiv x_2 \pmod 2$. For, otherwise, $x_1 \equiv x_3 \equiv x_2 + 1 \pmod 2$; then, according as x_1 is odd or even, the left member of (9) is $\equiv 2$ or $-1 \pmod 4$ and hence is not a square. Hence we may write

$$x = \frac{1}{2}(x_1 + x_2), \qquad y = x_2, \qquad z = \frac{1}{2}(x_4 + x_3), \qquad w = \frac{1}{2}(x_4 - x_3),$$

where x, y, z, w are integers. Then (9) reduces to (8) and is completely solved in integers. Hence *for $m = 1, 2, -2, 3, -3, -5, 7, 11, -13$, all the integral solutions of $x_1^2 + mx_2^2 + x_3^2 = x_4^2$ are given by a single formula obtained by the norm theorem.*

However, if we attempt to apply our method to find all the integral solutions of $x_1^2 + 5x_2^2 + x_3^2 = x_4^2$, and hence of

$$(10) \qquad x^2 + 5y^2 = zw,$$

we must take into account the fact that the numbers $x + y\theta$, where x and y are integers and $\theta = \sqrt{-5}$, do not obey the laws of divisibility of arithmetic. In fact, there are here two classes of ideals, one being composed of all the principal ideals and the other being composed of the ideals equivalent to a prime ideal factor of the principal ideal $\{2\}$. Thus in removing a common prime factor from the solutions

$$x = mn - 5rq, \qquad y = mr + nq, \qquad z = m^2 + 5q^2, \qquad w = n^2 + 5r^2$$

of (10), furnished by the norm theorem, the quotients need not be of this same form, but may be of a new form obtained by cancelling the common factor 2 from

$$2x = \mathrm{MN} - 5rq, \qquad 2y = \mathrm{M}r + \mathrm{N}q, \qquad 2z = \mathrm{M}^2 + 5q^2, \qquad 2w = \mathrm{N}^2 + 5r^2.$$

where $\mathrm{M} = 2m + q$, $\mathrm{N} = 2n + r$. In general, we obtain as many sets of formulas for the integral solutions as there are classes of ideals. We cannot enter here upon the details of this more technical application of our method, which will be published in a mathematical journal.

Moreover, our method is applicable to further types of equations such as $x_1^2 + \ldots + x_5^2 = x_0^2$, whose complete solution in integers is easily seen to reduce to that of

$$(11) \qquad x^2 + y^2 + z^2 + w^2 = \xi\eta.$$

We employ the theorem that the norm $x^2 + y^2 + z^2 + w^2$ of the product

$$(12) \qquad x + yi + zj + wk = \mathrm{AB}$$

of two quaternions

$$(13) \qquad \mathrm{A} = a + bi + cj + dk, \qquad \mathrm{B} = \alpha + \beta i + \gamma j + \delta k$$

equals the product of their norms. Thus (11) has the solutions

$$(14) \qquad \begin{cases} x = a\alpha - b\beta - c\gamma - d\delta, & y = a\beta + b\alpha + c\delta - d\gamma, \\ z = a\gamma - b\delta + c\alpha + d\beta, & w = a\delta + b\gamma - c\beta + d\alpha, \\ \xi = a^2 + b^2 + c^2 + d^2, & \eta = \alpha^2 + \beta^2 + \gamma^2 + \delta^2. \end{cases}$$

The products of an arbitrary rational number ρ by these six numbers (14), in which $a, \ldots, \delta$ are integers without a common factor, give all the rational solutions of (11), since this is readily verified to be the case when $\beta = \gamma = \delta = 0$ by the method used for (1). To show that all the integral solutions are obtained by multiplying the numbers (14) by integers ρ, it remains to prove that, if these numbers (14) are all divisible by a prime p, the quotients are expressible in the same form (14) with $a, \ldots, \delta$ replaced by new integral parameters.

On the proof, we shall need the fact, proved by A. Hurwitz [1], that there exists a right-hand (as well as a left-hand) greatest common divisor of any two integral quaternions. Here a quaternion is called integral if its four coordinates are either all integers or all halves of odd integers. The latter possibility would seem to present a difficulty [2] in applying such an arithmetic of quaternions to the study of the integral solutions of our Diophantine equation; but we shall see that this difficulty is easily overcome, partly by giving a separate treatment for the case $p = 2$.

Since the norm ξ of the quaternion A with integral coordinates was assumed to be divisible by the prime p ($p > 2$), and since p equals the product $PP' = P'P$ of two conjugate prime quaternions with integral coordinates, we have $A = QP$, after choice of the notation between P and P′. Here the integral quaternion Q must have integral coordinates, since otherwise $Q = \frac{1}{2}q$, where q has odd integral coordinates, and

$$AP' = \frac{1}{2}q \, . \, p = \frac{1}{2}p \, . \, q$$

would not have integral coordinates, in contradiction with the fact that A and P have integral coordinates.

Since x, y, z, w are by hypothesis divisible by p, we have $AB = pC$ by (12), where C has integral coordinates. Either B has P′ as a left-hand divisor, so that $B = P'q$, where as above q has integral coordinates, or else the left-hand greatest common divisor of B and P′ is unity, so that $1 = BD + P'E$, where D and E are integral quaternions. In the latter case,

$$A = A \, . \, BD + A \, . \, P'E = pC \, . \, D + Q(PP')E = p(CD + QE),$$

where $CD + QE$ is an integral quaternion, so that its double is a quaternion R with integral coordinates. Hence $2A = pR$, whereas the coordinates of A may be assumed to be not all divisible by p. For, if a, b, c, d are all divisible by p, then $\alpha, \beta, \gamma, \delta$ are not all divisible by p and me may employ from the outset the conjugate B′A′

[1] *Göttingen Nachrichten*, 1896, pp. 311-340.

[2] A second method is to restrict the term integral quaternion to one whose coordinates are all integers. A quaternion whose norm is odd is called an odd quaternion. I have succeeded in obtaining a direct prooof of the fact that any two integral quaternions A and B, at least one of which is odd, have a right-hand greatest common divisor D which is uniquely determined up to a unit factor (± 1, $\pm i$, $\pm j$, $\pm k$), and that $D = EA + FB$, where E and F are integral quaternions. The further theory proceeds as with Hurwitz.

of AB in place of AB. Hence we have the first case $B = P'q$. Thus

$$A = QP, \quad Q = a_1 + b_1 i + c_1 j + d_1 k, \quad \xi = N(A) = p(a_1^2 + \ldots + d_1^2),$$
$$B = P'q, \quad q = \alpha_1 + \beta_1 i + \gamma_1 j + \delta_1 k, \quad \eta = N(B) = p(\alpha_1^2 + \ldots + \delta_1^2),$$

where N(A) denotes the norm of A. By multiplication,

$$AB = QPP'q = pQq.$$

By comparaison with (12), we see that x/p, y/p, z/p, w/p, ξ/p, η/p are of the form (14) with $a, \ldots \delta$ replaced by the eight new integral parameters $a_1, \ldots, \delta_1$. This completes the proof for any odd prime p.

Next, let $p = 2$. Since ξ is divisible by 2, $a + b + c + d$ is even. Hence at least one of $a + b$, $a + c$, $a + d$ is even. These three cases differ only in notation since the substitution $T = (b\,c\,d)\,(\beta\,\gamma\,\delta)\,(y\,z\,w)$ leaves the system of equations (14) unaltered [1]. Hence we may assume that $a + b$ is even, so that $c + d$ is even. Since

$$A = a - b + b(1 + i) + (c - d)j + dk(1 + i), \qquad 2 = (1 - i)(1 + i),$$

$A = QP$, where $P = 1 + i$ and Q has integral coordinates. Similarly, if $\alpha + \beta$ is even, $B = P'q$ and the final part of the proof given above for $p > 2$ yields the same result here. But if $\alpha + \beta$ is odd, $\gamma + \delta$ is odd and either $\alpha + \gamma$ or $\alpha + \delta$ is even. These sub-cases are interchanged when we replace a by b, b by $-a$, γ by $-\delta$, and δ by γ, whence z and w remain unaltered, while x is replaced by y, and y by $-x$. Hence let $\alpha + \gamma$ be even. Since also $a + b$ and $c + d$ are even, while $\alpha + \beta$ and $\gamma + \delta$ are odd, we have

$$0 \equiv x \equiv a\alpha + a(\alpha + 1) - c\gamma + c(\gamma + 1) \equiv a + c \pmod 2.$$

Applying the inverse substitution T^{-1}, we are led to the former case in which $a + b$ and $\alpha + \beta$ are even.

Thus *all the integral solutions of (11) are given by the producls of the numbers* (14) *by an arbitrary integer, and hence are given by the formula which expresses the fact that the norm of the product of two quaternions equals the product of their norms.*

[1] This is due to the fact that T corresponds to the cyclic substitution $(i\,j\,k)$ on the units, which leaves unaltered their multiplication table.

III. Modular invariants.

I shall indicate briefly and concretly the nature of modular invariants, the theory of which has been investigated extensively in the United States in recent years [1]. In what follows, p denotes a prime number. Lagrange proved that all of the coefficients in the expansion of

$$x^p - x - x(x+1)(x+2)\dots(x+p-1)$$

are divisible by p, and deduced the well-known theorems of Fermat and Wilson. By replacing x by x/y, we may express Lagrange's theorem in the homogeneous form

$$(1) \qquad \begin{vmatrix} x^p & y^p \\ x & y \end{vmatrix} \equiv y \prod_{k=0}^{p-1} (x+ky) \quad (\text{mod } p).$$

The right member is the product of all the incongruent linear forms having unity as leading coefficients. Apart from numerical factors, these linear forms are evidently merely permuted by any linear substitution

$$(2) \qquad x = ax_1 + by_1, \qquad y = cx_1 + dy_1,$$

with integral coefficients, provided we omit multiples of p. Hence their product (1) is a (relative) invariant modulo p. We can prove independently that the determinant is a relative invariant modulo p. For, since $a^p \equiv a$ (mod p), (2) gives

$$x^p \equiv ax_1^p + by_1^p, \qquad y^p \equiv cx_1^p + dy_1^p \qquad (\text{mod } p),$$

$$\begin{vmatrix} x_1^p & y_1^p \\ x_1 & y_1 \end{vmatrix} \cdot \begin{vmatrix} a & c \\ b & d \end{vmatrix} \equiv \begin{vmatrix} x^p & y^p \\ x & y \end{vmatrix} \qquad (\text{mod } p).$$

Since the determinant is an invariant having the factor y, it has as a factor every linear form, since our substitutions replace y by each linear form. Finally, each member of (1) contains the term x^py with the coefficient unity. This completes the proof that (1) is a congruencial identity.

Evidently the same argument leads to the generalization

$$(3) \qquad \begin{vmatrix} x^{p^2} & y^{p^2} & z^{p^2} \\ x^p & y^p & z^p \\ x & y & z \end{vmatrix} \equiv z \prod_{k=0}^{p-1} (y+kz) \cdot \prod_{l,m=0}^{p-1} (x+ly+mz) \quad (\text{mod } p).$$

[1] References to the literature down to 1913 are given in the writer's *Madison Colloquium Lectures*, American Mathematical Society, 1914.

and to the corresponding congruencial identity in n variables. The earliest proof of these results did not employ modular invariants and was quite complicated.

Returning to the case of two variables, we note that also

$$(4) \qquad \begin{vmatrix} x^{p^2} & y^{p^2} \\ x & y \end{vmatrix}$$

is an invariant modulo p. It is congruent to the product of all the incongruent linear and irreducible quadratic forms having unity as leading coefficients. We omit the proof, which employs the imaginaries of Galois. The quotient Q of (4) by the product L of the linear forms (1) is therefore a modular invariant.

It is superfluous to consider similarly the products of the irreducible cubic forms, quartic forms, etc., sinçe it can be readily proved that L and Q form a fundamental system of binary invariants modulo p. On the contrary, we can deduce important conclusions concerning cubic and higher forms by means of the invariants

$$l = \mathrm{L}^{p(p-1)/d}, \quad q = \mathrm{Q}^{(p+1)/d} \qquad (d = 2 \text{ if } p > 2, \quad d = 1 \text{ if } p = 2),$$

in terms of which we can express the product π_m of all the binary forms $x^m + \ldots$ which are irreducible modulo p. For $p > 2$, we have $\pi_3 = q^2 - l^2$, so that irreducible cubic factors of $q - l$ are all equivalent, as are also those of $q + l$, while no factor of $q - l$ is equivalent to a factor of $q + l$; here two forms are called equivalent if one of them can be transformed into a constant multiple of the other modulo p by a linear substitution with integral coefficients of determinant unity.

There are similar invariantive criteria for the equivalence of two irreducible forms of any degree. For forms in m variables, a great variety of analogous theorems have been established by means of the m fundamental invariants, one of which is the generalization of determinants (1) and (3), and the others are obtained by dividing it into determinants generalizing (4).

Hitherto I have spoken only of the modular invariants of a group. However, there is the larger subject of the invariants and covariants modulo p of any ground form or system of ground forms; these modular covariants evidently include all the algebraic covariants of the ground forms. The modular invariants of which I was speaking in detail are merely the universal covariants, in the same sense as $u_1x_1 + u_2x_2 + \ldots$ in the algebraic theory.

A simple, complete theory of the modular invariants of any system of forms has been constructed by means of the theory of classes of forms under linear transformations of determinant unity. For example, if $p > 2$, all binary quadratic forms which are congruent to squares of linear forms modulo p form a class with the representative form x^2. Again, there is a class represented by νx^2, where ν is a particular quadratic non-residue of p. Also, for $D = 1, 2, \ldots, p - 1$, there are classes represented by $x^2 + Dy^2$. Finally, there is the class of forms all of whose coefficients are divisible by p. A single-valued function of the coefficients of the general binary quadratic form f is a modular invariant of f if and only if the function has the same value modulo p for all the forms in the class represented by x^2, the same (new) value for all the forms in the class represented by νx^2, and so on for each of the $p + 2$ classes. The number of linearly independent modular invariants is always equal to the number of classes. The theory based upon classes is far simpler than a theory based upon methods in vogue for algebraic invariants. In the modular theory, the group of linear transformations is used solely to separate the classes, and is not used to furnish any test for invariance.

IV. Algebraic invariants.

There is an interesting application by Mordell [1] of the theory of algebraic invariants to the problem of finding the integers x and y for which a given binary cubic form shall equal a square. We take the cubic in the reduced form

$$4x^3 - g_2xy^2 - g_3y^3 = z^2. \tag{1}$$

This form was suggested by the syzygy

$$4h^3 - g_2ha^2 - g_3a^3 = g^2 \tag{2}$$

which connects the invariants g_2 and g_3 of the quartic

$$f = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4,$$

and its seminvariants $a, h = b^2 - ac, g = a^2d - b^3 + 3bh$. Given integral solutions of (2) in which a is odd and relatively prime to h $(h \neq 0)$, we can find integers $a, \ldots, e$ such that f has the invariants g_2 and g_3, and such that b is prime to a. The converse is evidently true. Hence to find all solutions of (1) in which y is odd and prime to x, we take a representative f of each of the classes (finite [2] in number) of binary quartics with integral coefficients and assigned values of the invariants g_2 and g_3; then apply to f such a linear substitution $\begin{pmatrix} p & r \\ q & s \end{pmatrix}$ with integral coefficients of determinant unity that we obtain a new quartic f' for which a' is odd and prime to b', whence

$$y = a' = f(p, q), \qquad x = h' = -H(p, q).$$

[1] *Quar. Jour. Math.*, t. 45, 1914, pp. 170-186.

[2] Hermite, *Jour. für Math.*, vols. 36, 41, 52; *Œuvres*, I, pp. 84, 164, 350.

where H is the Hessian of f. Hence the complete solution of (1) in relatively prime integers x, y is given by a finite number of pairs of quartic forms in two parameters p, q.

Mordell discussed also the solution of $f = w^2$, where f is a binary quartic with the invariants g_2 and g_3, under the assumption that one set of rational solutions is given. Then we can evidently transform f into a quartic whose leading coefficient is w^2. The syzygy (2) becomes

$$4h^3 - g_2hw^4 - g_3w^6 = g^2,$$

so that $s = h/w^2, t = g/w^3$ give rational solutions of

$$4s^3 - g_2s - g_3 = t^2.$$

He proved that a knowledge of all the rational solutions of the latter cubic leads to all the rational solutions of the quartic $f = w^2$.

This method may be applied to find the rational solutions of $F = 0$, given one solution, where F is a ternary cubic form. By means of a linear substitution with rational coefficients of determinant unity, we can transform $F = 0$ into

$$S_1\xi^2 + 2S_2\xi + S_3 = 0,$$

where S_j is a function of η, φ of degree j. The discriminant $f = S_2^2 - S_1S_3$ is a binary quartic whose invariants are numerical multiples of the invariants S and T of F. If $S_1 = b\eta + c\varphi$, then f is a square S_2^2 for $\eta = -c$, $\varphi = b$. Hence if we can find all the rational solutions of

$$4s^3 + 108Ss - 27T = t^2,$$

we can deduce all the rational solutions of $F = 0$.