A DIOPHANTINE AUTOMORPHISM*

BY E. T. BELL

1. *Introduction.* We define a *diophantine automorphism* of a form $f \equiv f(x, y, \cdots, w)$ to be a transformation of f into f^n, where $n > 1$ is an integer, by means of a substitution of the type

$$x = X(x, y, \cdots, w), \qquad y = Y(x, y, \cdots, w), \cdots,$$
$$w = W(x, y, \cdots, w),$$

so that

$$f(X, Y, \cdots, W) = f^n(x, y, \cdots, w),$$

where $X, Y, \cdots, W$ are rational integral functions, with rational integral coefficients, of $x, y, \cdots, w$ and the coefficients of f.

Obviously powers of norms of algebraic integers, powers of sums of 4 or 8 squares, the generalizations of the latter which are composable forms and, generally, any power greater than the first of any composable form, have the automorphic property just defined. Excluding powers of composable forms we shall call any other form having a diophantine automorphism *proper*.

Examples of proper forms are extremely rare; their interest for diophantine analysis is evident. Apparently there are known but two instances, the discriminant of a binary cubic, this observation being due to Eisenstein† (see §9), and Cayley's‡ generalization of this to a certain octenary quartic with numerical coefficients $(1, -2, 4)$.

Being given a proper automorphism for a form with numerical coefficients, we devise a method of generalization

* Presented to the Society, San Francisco Section, October 30, 1926.

† F. M. G. Eisenstein, Crelle's Journal, vol. 27 (1844), p. 105.

‡ A. Cayley, Collected Mathematical Papers, vol. 1, pp. 89–91; p. 113; p. 353; p. 532.

which yields a proper form with literal coefficients, whose automorphism degenerates to that of the given form when each of the literal coefficients is replaced by unity. The method leads to systems of linear diophantine equations and inequalities whose solution gives the required generalization. Both Eisenstein's and Cayley's automorphisms can be generalized in this way. The ordinary diophantine problem for Cayley's is so complicated, however, (leading as one detail to a system of 76 equations and inequalities in 8 variables), that we shall reproduce here only the work for Eisenstein's. The method extends and systematizes that used in a former paper* to generalize the 8 square identity, and it is applicable to all problems discussed there.

2. *Matric Exponents and Multipliers of a Transformation.* Let a, b, c be constant integers >0, and $u_j, v_j, r_j (j=1, \cdots, g)$ variable integers $\geqq 0$. Let $\phi_j (j=1, \cdots, g)$ be independent parameters. Write, symbolically,

$$\prod_{j=1}^{g} \phi_j^{au_j} \equiv \phi^{au},$$

and call au the *matric exponent* of ϕ. Let ϕ^{au}, ϕ^{bv}, ϕ^{cr} be any three such symbolic powers between which there is the relation

$$\phi^{au}\phi^{bv} = \phi^{cr},$$

the indicated multiplication on the left being as in common algebra, so that

$$au_j + bv_j = cr_j, \qquad (j = 1, \cdots, g).$$

Then we shall write these g equations as the single equation

$$au + bv = cr$$

between matric exponents, and similarly for matric equations in any number of variables $u, v, r, s, \cdots, x$.

The laws of combination of such equations are abstractly identical with those for ordinary linear systems, being merely a translation of the laws of algebraic exponents. It is unneces-

* E. T. Bell, Annals of Mathematics, (2), vol. 27 (1925), p. 99.

sary to elaborate them formally as they will be clear from the application made later.

Let $x, y, \cdots, z$ be independent variables, and $a, b, \cdots, c, u, v, \cdots, r, \phi$ as before. Then $\phi^{au}, \phi^{bv}, \cdots, \phi^{cr}$ will be called the *multipliers* of the transformation which replaces $x, y, \cdots, z$ by $\phi^{au}x, \phi^{bv}y, \cdots, \phi^{cr}z$ respectively.

In generalizing automorphisms we deal with a great many multipliers, matric exponents and variables simultaneously, and it is a saving of labor, also a suggestive impulse to the algebra to use a device which will show at a glance the specific variable to which a given exponent or multiplier appertains.

We shall write $\phi^x, \phi^y, \cdots, \phi^z$ for the multipliers appertaining to the variables $x, y, \cdots, z$. The exponents of these multipliers are $x, y, \cdots, z$. Finally, the multipliers will be denoted by their exponents. Thus $x, y, \cdots, z$ will denote either variables, the respective multipliers of these variables, or the matric exponents of the latter. No confusion can result from this triple interpretation of $x, y, \cdots, z$, as in each case it will be stated what the letters are. This supple device enables us to follow the multiplicative transformations of a set of variables without elaborate notations and with a minimum of algebra. It also reduces the particular kind of diophantine problem occurring in the subject from degree $n>1$ to degree 1.

3. *Eisenstein's Automorphism.* As we start from Eisenstein's identity we transcribe it here. Write

$$f(x,y,z,w) \equiv x^2w^2 - 3y^2z^2 + 4xz^3 + 4wy^3 - 6xyzw,$$
$$X \equiv 3xyz - x^2w - 2y^3$$
$$Y \equiv 2xz^2 - xyw - y^2z,$$
$$Z \equiv xzw - 2y^2w + yz^2,$$
$$W \equiv xw^2 - 3yzw + 2z^3,$$

so that

$$X = -\frac{1}{2}\frac{\partial f}{\partial w}, \quad Y = \frac{1}{6}\frac{\partial f}{\partial z}, \quad Z = -\frac{1}{6}\frac{\partial f}{\partial y}, \quad W = \frac{1}{2}\frac{\partial f}{\partial x}.$$

The automorphism is then

$$f(X,Y,Z,W) = f^3(x,y,z,w).$$

This striking result is today evident in many ways, for example by observing the discriminant of the cubicovariant of the binary cubic of which $f(x, y, z, w)$ is the discriminant. Nevertheless Eisenstein's remarks on it still stand, as no proof has indicated a method of attack on the general problem of finding all composable forms or upon the equally (or more) difficult one of diophantine automorphism which his theorem illustrates, and of which it was the first example. He says:

"Es scheint, man müsse dieser Gattung von identischen Gleichungen eine um so grössere Wichtigkeit zuschreiben, als man keine allgemeine Methode zu ihrer Auffindung besitzt, und weil dieselben namentlich in der Zahlenlehre oft die Grundlage zu ganzen Theorieen bilden; in welcher Hinsicht sich auf die Theorieen der quadratischen und ternären Formen, so wie auf diejenige der Zerlegung einer Zahl in die Summe von vier Quadraten und andere verweisen lasst."

It was proved by Dickson* that f is proper in the sense of §1.

4. *Summary of Extension.* We put here for convenience, in ordinary notation, the conclusion which follows from the subsequent algebra in §8. Let ϕ_j $(j=1, \cdots, g)$ be parameters, l_j, m_j, n_j, r_j arbitrary integers $\geqq 0$, such that

$$2m_j = l_j + n_j + r_j, \qquad (j = 1, \cdots, g),$$

and write

$$\lambda \equiv \prod_{j=1}^{g} \phi_j^{l_j}, \qquad \mu \equiv \prod_{j=1}^{g} \phi_j^{m_j}, \qquad \nu \equiv \prod_{j=1}^{g} \phi_j^{n_j},$$

$$\rho \equiv \prod_{j=1}^{g} \phi_j^{r_j}.$$

Then

$$[\mu^2(\lambda xw - yz)^2 - 4\lambda(\mu xz - \rho y^2)(\mu yw - \nu z^2)]^3$$
$$= \mu^2(\lambda XW - YZ)^2 - 4\lambda(\mu XZ - \rho Y^2)(\mu YW - \nu Z^2),$$

* L. E. Dickson, Comptes Rendus du Congrès International des Mathématiciens, Strassbourg, 1921, (pub. Toulouse): *Homogeneous polynomials with a multiplication theorem*, §9. The property of the Hessian noted by Haskell, American Mathematical Monthly, vol. 10 (1903) p. 2 and cited by Dickson, loc. cit., p. 9, was first proved by Cayley.

where

$$X \equiv 3\mu xyz - \lambda\mu x^2w - 2\rho y^3,$$
$$Y \equiv 2\lambda\nu xy^2 - \lambda\mu xyw - \mu y^2z,$$
$$Z \equiv \lambda\mu xzw - \lambda\rho y^2w + \mu yz^2,$$
$$W \equiv \lambda\mu xw^2 - 3\mu yzw + 2\nu z^3.$$

For $0=l_j=m_j=n_j=r_j$ $(j=1, \cdots, g)$ this becomes Eisenstein's identity in §3. An alternative form of the above is

$$\lambda^2[\nu\rho(\lambda xw - yz)^2 - 4(\mu xz - \rho y^2)(\mu yw - \nu z^2)]^3$$
$$= \nu\rho(\lambda XW - YZ)^2 - 4(\mu XZ - \rho Y^2)(\mu YW - \nu Z^2),$$

where λ, μ, ν, ρ are any parameters subject only to the condition

$$\mu^2 = \lambda\nu\rho.$$

For these parameters we have in fact

$$\mu^2(\lambda xw - yz^2) - 4\lambda(\mu xz - \rho y^2)(\mu yw - \nu z^2)$$
$$= \lambda[\nu\rho(\lambda xw - yz)^2 - 4(\mu xz - \rho y^2)(\mu yw - \nu z^2)],$$

and obviously the original λ, μ, ν, ρ (in terms of the ϕ_i) satisfy $\mu^2=\lambda\nu\rho$.

Although it is not of the type discussed in this paper, we may note in passing the following curious identity:

$$(px^2w^2 - 3qy^2z^2 + 4rxz^3 + 4swy^3 - 6txyzw)^3$$
$$= \frac{1}{p}X^2W^2 - \frac{3}{q}Y^2Z^2 + \frac{4}{r}XZ^3 + \frac{4}{s}WY^3 - \frac{6}{t}XYZW,$$

where

$$X \equiv 3txyz - px^2w - 2sy^3,$$
$$Y \equiv 2rxz^2 - txyz - qy^2z,$$
$$Z \equiv txzw - 2sy^2w + qyz^2,$$
$$W \equiv pxw^2 - 3tyzw + 2rz^3,$$

and p, q, r, s, t are any parameters such that

$$(pq - t^2)(rs - qt) = 0.$$

This is a consequence of either set of formulas in §§ 3, 4.

5. *Transformation of f.* Transform f in §3 by

$$\Sigma \equiv \begin{pmatrix} x, & y, & z, & w \\ x\phi^x, & y\phi^y, & z\phi^z, & w\phi^w \end{pmatrix},$$

the exponents of ϕ being matric, into

$$F \equiv Px^2w^2 - 3Qy^2z^2 + 4Rxz^3 + 4Swy^3 - 6Txyzw$$

and let the respective matric exponents of P, Q, R, S, T be p, q, r, s, t. Then

$$\begin{aligned} p &= 2x + 2w, \\ q &= 2y + 2z, \\ r &= x + 3z, \\ s &= w + 3y \\ t &= x + y + z + w, \end{aligned} \tag{1}$$

a set of diophantine matric equations.

Under Σ the matric exponents of the respective terms, in the order in which they occur, in X, Y, Z, W of §3 are

$$\begin{array}{lll} x + y + z\ , & 2x + w, & 3y, \\ x + 2z, & x + y + w, & 2y + z, \\ x + z + w\ , & 2y + w, & y + 2z, \\ x + 2w, & y + z + w\ , & 3z, \end{array} \tag{2}$$

and the multipliers having these respective exponents are

$$\begin{array}{lll} xyz\ , & x^2w\ , & y^3\ , \\ xz^2\ , & xyw\ , & y^2z\ , \\ xzw\ , & y^2w\ , & yz^2\ , \\ xw^2\ , & yzw\ , & z^3\ . \end{array} \tag{3}$$

6. *Conditions for Diophantine Automorphism.* As in the theory of numbers, if a, b, c, $\cdots$ are integral elements of any ray, and the quotient of b by a is an element of the ray, say c, we write $a \mid b$ for "a divides b." Hence $a \mid b$ implies that there exists an integral element c such that $b = ac$. Note that we are concerned throughout with arithmetic division and not merely algebraic. As in algebra a/b is the result of dividing a by b.

In order that F of §5 shall have a diophantine automorphism it is sufficient by (3) that the following 12 relations of divisibility for multipliers shall subsist,

$$(4)\qquad \begin{aligned} x &\mid (xyz,\ x^2w,\ y^3),\\ y &\mid (xz^2,\ xyw,\ y^2z),\\ z &\mid (xzw,\ y^2w,\ yz^2),\\ w &\mid (xw^2,\ yzw,\ z^3). \end{aligned}$$

Passing from (4) to matric exponents we see that the following must be integers $\geqq 0$:

$$(5)\qquad \begin{array}{lll} y+z, & x+w, & 3y-x,\\ x+2z-y, & x+w, & y+z,\\ x+w, & 2y+w-z, & y+z,\\ x+w, & y+z, & 3z-w. \end{array}$$

Hence it is sufficient that the following inequalities shall hold in integers (matric exponents) $\geqq 0$,

$$(6)\qquad 3y \geqq x, \quad x+2z \geqq y, \quad w+2y \geqq z, \quad 3z \geqq w.$$

The problem is therefore reduced to satisfying (1), (6) in integers $x, y, z, w, p, q, r, s, t \geqq 0$, the general solution being required.

7. *Solution of* (1), (6). From (1) we have

$$(7)\qquad p+q=2t, \qquad r+s=q+t,$$

and hence from (1)

$$(8)\qquad \begin{aligned} 6y &= 2x+2s-p,\\ 3z &= r-x,\\ 2w &= p-2x,\\ 3q &= 2r+2s-p,\\ 3t &= r+s+p, \end{aligned}$$

which must be solved in integers $\geqq 0$ subject to (6).

Treat x, r, p, s as parameters. Then, for integrality we must have

$$\begin{aligned} 2x + 2s &\equiv p, && \text{mod } 6, \\ r &\equiv x, && \text{mod } 3, \\ p &\equiv 0, && \text{mod } 2, \\ 2r + 2s &\equiv p, && \text{mod } 3, \\ r + s + p &\equiv 0, && \text{mod } 3. \end{aligned} \tag{9}$$

From the first of (9) we get $p \equiv 0, \text{mod } 2$; hence the third is redundant. Now if $p = 2k$, then $p \equiv 4p$, mod 6, and hence from the first, $2x+2s \equiv 4p$, mod 6; thus, by the second, $r+s \equiv 2p$, mod 3, and this implies the fifth. The set (9) is therefore equivalent to

$$2x + 2s \equiv p, \quad \text{mod } 6, \qquad r \equiv x, \quad \text{mod } 3\,; \tag{10}$$

and from (6), (8) we get

$$2r \geqq p, \quad 2s \geqq p, \quad 4r + p \geqq 2s, \quad 4s + p \geqq 2r \tag{11}$$

and we have also

$$q = (2r + 2s - p)/3, \qquad t = (r + s + p)/3. \tag{12}$$

The array (5) now becomes

$$\begin{array}{lll} (2r - p + 2s)/6, & p/2, & (-p + 2s)/2, \\ (4r + p - 2s)/6, & p/2, & (2r - p + 2s)/6, \\ p/2, & (-2r + p + 4s)/6, & (2r - p + 2s)/6, \\ p/2, & (2r - p + 2s)/6, & (-p + 2r)/2. \end{array} \tag{13}$$

If (10), (11) are satisfied, it follows from the way in which (13) was obtained that its 12 members are integers $\geqq 0$. To exhibit this solution in terms of ordinary algebra we make some reductions.

8. *Transition to Ordinary Algebra.* By §5, beginning, we have

$$(P, Q, R, S, T) = (\phi^p, \phi^q, \phi^r, \phi^s, \phi^t)\,;$$

hence the equivalent in terms of multipliers of (13) is

$$(14)\qquad \begin{matrix} (R^2S^2/P)^{1/6}, & P^{1/2}, & (S^2/P)^{1/2}, \\ (PR^4/S^2)^{1/6}, & P^{1/2}, & (R^2S^2/P)^{1/6}, \\ P^{1/2}, & (PS^4/R^2)^{1/6}, & (R^2S^2/P)^{1/6}, \\ P^{1/2}, & (R^2S^2/P)^{1/6}, & (R^2/P)^{1/2}, \end{matrix}$$

and from (12) we have

$$(15)\qquad Q = (R^2S^2/P)^{1/3}, \qquad T = (PRS)^{1/3},$$

and P, R, S are not similarly reducible, since we took x, p, r, s as independent (matric) parameters.

As a check, we should have, by (7),

$$(16)\qquad (PQ - T^2)(RS - QT) = 0,$$

a relation used in what follows, and this is verified by (15).

Applying (16) to (14), we get the array in the form

$$(17)\qquad \begin{matrix} Q^{1/2}, & P^{1/2}, & S/P^{1/2}, \\ R/Q^{1/2}, & P^{1/2}, & Q^{1/2}, \\ P^{1/2}, & S/Q^{1/2}, & Q^{1/2}, \\ P^{1/2}, & Q^{1/2}, & R/P^{1/2}, \end{matrix}$$

whose twelve members must be rational integral functions of parameters together with Q, T as given by (15).

For rationality and integrality (17) demands

$$(18)\qquad Q = Q_1^2, \quad P = P_1^2, \quad S = S_1P_1 = S_2Q_1, \quad R = R_1Q_1 = R_2P_1,$$

the letters with suffixes being new parameters. From (18) we get

$$(19)\qquad Q_1^6\,P_1^2 = R^2S^2, \qquad T^3 = RSP_1^2, \qquad P_1/Q_1 = S_2/S_1 = R_1/R_2 = K,$$

where K is a new parameter. Hence

$$(20)\qquad P = K^2Q_1^2, \quad Q = Q_1^2, \quad R = KQ_1R_2, \quad S = KQ_1S_1, \quad T = KQ_1^2,$$

expressing P, Q, R, S, T in terms of 4 parameters K, Q_1, R_2, S_1 between which is the single relation

$$Q_1^2 = KR_2S_1. \tag{21}$$

Finally then, making the change in notation

$$\lambda \equiv K, \qquad \mu \equiv Q_1, \qquad \nu \equiv R_2, \qquad \rho \equiv S_1,$$

we have the results summarized in §§ 3, 4.

The use of the symbolic method is a rapid means for proving the existence or non-existence of a diophantine automorphism; the passage to ordinary algebra is then a simple translation of the matric and multiplier equations of the symbolic solution. Notice that the symbolic method avoids all irrationalities; its equations and all of its processes are carried out in terms of positive integers.

9. *References.* Many of Cayley's papers contain references to Eisenstein's theorem and to his own generalization of it, including the geometry of the related developable surface in homogeneous coordinates. Cayley's form is of interest from another point of view; it is that (an octenary quartic) which occurs incidentally in section 235 of the *Disquisitiones Arithmeticae* in connection with the composition of binary quadratic forms.

CALIFORNIA INSTITUTE OF TECHNOLOGY