THE FUNCTIONAL EQUATION DEFINING DIOPHANTINE AUTOMORPHISMS*

BY LOUIS WEISNER†

1. *Introduction*. A form $f(x_1, \cdots, x_m)$ is said to admit a *diophantine automorphism* if there exist m forms

$$\phi_1(x_1, \cdots, x_m), \cdots, \phi_m(x_1, \cdots, x_m),$$

such that

$$(1) \qquad f[\phi_1(x_1, \cdots, x_m), \cdots, \phi_m(x_1, \cdots, x_m)] = f^n(x_1, \cdots, x_m),$$

where n is a positive integer greater than 1, the coefficients of the forms being integers or rational integral functions of one or more parameters with integral coefficients. In view of Bell's remarks (*A diophantine automorphism*, this Bulletin, vol. 28, p. 71) on the scarcity of what he calls *proper* diophantine automorphisms, it seems desirable to seek solutions of (1), regarded as a functional equation, no restrictions being placed on the algebraic nature of the solution or the coefficients.

Three methods of obtaining solutions of this functional equation are offered in the present paper. The first method gives a solution corresponding to any one-parameter continuous group having certain properties. The solution is generally a transcendental function, but I present this method here as the functional equation is of interest in analysis. In the second method f is assumed known, and the ϕ's are to be determined. It is shown that if there exists a Cremona transformation of which $x_i' = f(x_1, \cdots, x_m)$ is a constituent, then there exist *rational* functions $\phi_1, \cdots, \phi_m$ satisfying (1). This leads to rational solutions of the diophantine equation

$$f(x_1, \cdots, x_m) = u^n.$$

* Presented to the Society, May 7, 1927.

† National Research Fellow.

The third method is more satisfactory for the purposes of diophantine analysis. It is shown that if the ϕ's are forms such that the equations

$$x_i' = \phi_i(x_1, \cdots, x_m), \qquad (i = 1, \cdots, m),$$

define a Cremona transformation of finite period, then there exists a form $f(x_1, \cdots, x_m)$ satisfying (1). Eisenstein's automorphism is obtained in this way. A diophantine automorphism may be obtained from every Cremona transformation of finite period, but not every diophantine automorphism may be obtained in this way. For example, the transformation

$$x_1' = x_1^n, \cdots, x_m' = x_m^n$$

is not a Cremona transformation, but it transforms $x_1 x_2 \cdots x_m$ into its nth power.

2. *First Method. One-Parameter Groups.* Let

$$x_i' = \phi_{it}(x_1, \cdots, x_m), \qquad (i = 1, \cdots, m) \tag{2}$$

be a one-parameter continuous group (t being the parameter) analytic in the neighborhood of $t=0$ and in some region of the x-space. The variables are non-homogeneous. We assume that the parameter of the product of two transformations of the group equals the sum of the parameters of the transformations, and that the identical transformation is given by $t=0$.*

Instead of (1) we consider

$$f(\phi_{1t}, \cdots, \phi_{mt}) = f^{n^t}(x_1, \cdots, x_m), \tag{3}$$

which reduces to (1) when $t=1$. Taking the logarithms of both members of (3) we obtain

$$g(\phi_{1t}, \cdots, \phi_{nt}) = n^t g(x_1, \cdots, x_m), \tag{4}$$

where

$$g(x_1, \cdots, x_m) = \log f(x_1, \cdots, x_m). \tag{5}$$

* See A. Cohen, *The Lie Theory of One-Parameter Groups*, §4.

Differentiating (4) with respect to t, and then putting $t=0$, we obtain

$$Ug(x_1, \cdots, x_m) = g(x_1, \cdots, x_m) \log n, \tag{6}$$

where U denotes the linear differential operator defining the infinitesimal transformation of the group (2). From (6) we deduce that

$$U^p g = g^p \log n.$$

Hence

$$\begin{aligned} g[\phi_{1t}, \cdots, \phi_{mt}] &= g + tUg + \frac{t^2}{2!}U^2 g + \cdots \\ &= g + tg \log n + \frac{t^2}{2!} \log^2 n + \cdots \\ &= gn^t. \end{aligned}$$

It follows that every solution of (6) is a solution of (4) which leads to a solution of (3) through the medium of (5). Now (6) is a linear partial differential equa ion of Lagrange's type which may be solved by the usual methods, the solution involving an arbitrary function. A solution of (1) may thus be obtained from any continuous group satisfying the stated conditions.

3. *Second Method. Arbitrary Transformations.* If

$$x_i' = f_i(x_1, \cdots, x_m), \qquad (i = 1, \cdots, m), \tag{7}$$

the variables being again non-homogeneous, is a reversible, but otherwise arbitrary transformation, the equations

$$f_i(x_1', \cdots, x_m') = F_i(x_1, \cdots, x_m), \quad (i = 1, \cdots, m), \tag{8}$$

where F_i is arbitrary, can be solved for $x_1', \cdots, x_m'$, giving, say,

$$x_i' = G_i(x_1, \cdots, x_m), \qquad (i = 1, \cdots, m). \tag{9}$$

Evidently

$$f_i(G_1, \cdots, G_m) = F_i(x_1, \cdots, x_m), \quad (i = 1, \cdots, m). \tag{10}$$

Regarding (10) as a system of functional equations in which $G_1, \cdots, G_m$ are the unknowns, a solution is provided by (9). If $h<m$ equations of the type (10) are given, we add $m-h$ other equations and obtain a solution involving $m-h$ arbitrary functions. Thus to find solutions of (1), f being given, select $m-1$ arbitrary functions $f_2, \cdots, f_m$, such that (7) is reversible ($f_1 \equiv f$), and let $F_2, \cdots, F_m$ be arbitrary functions. We obtain a solution involving $F_2, \cdots, F_m$.

Where f is a given *rational* function it is not always possible to find functions $f_2, \cdots, f_m$ such that $\phi_1, \cdots, \phi_m$ are rational. This will be the case, however, if (7) is a Cremona transformation, one of whose right members is f.

4. *An Example.* Applying the method of §3 to the equations

$$x' = \frac{x}{x^2+y^2}, \qquad y' = \frac{y}{x^2+y^2},$$

defining an inversion, we obtain the equations

$$\frac{x'}{x'^2+y'^2} = \left(\frac{x}{x^2+y^2}\right)^n, \qquad \frac{y'}{x'^2+y'^2} = F,$$

where F is an arbitrary rational function of x and y. Solving for x' and y', we obtain

$$x' = \frac{x^n(x^2+y^2)^n}{x^{2n}+(x^2+y^2)^{2n}F^2},$$
$$y' = \frac{(x^2+y^2)^nF}{x^{2n}+(x^2+y^2)^{2n}F^2}.$$

We readily verify that this transformation transforms $x/(x^2+y^2)$ into its nth power.

5. *Third Method. Finite Cremona Transformations.* The variables in (1) are now assumed homogeneous and

$$x_i' = \phi_{i1} \equiv \phi_i(x_1, \cdots, x_m), \qquad (i = 1, \cdots, m),$$

the ϕ's being forms of order n, are assumed to define a Cremona transformation of finite period p. The rth iterate of the ordered functions $\phi_{11}, \cdots, \phi_{m1}$ is denoted by $\phi_{1r}, \cdots, \phi_{mr}$, so that

$$\phi_{i0}(x_1, \cdots, x_m, \equiv x_i,$$

$$\phi_{ir}(x_1, \cdots, x_m) \equiv \phi_{i,r-1}(\phi_{11}, \cdots, \phi_{m1}).$$

Evidently

$$\phi_{1p}:\phi_{2p}: \cdots :\phi_{mp} = x_1:x_2: \cdots :x_m.$$

Since ϕ_{ip} is a form of order n^p, there exists a form $\psi(x_1, \cdots, x_m)$ of order $n^p - 1$ such that

$$x_i\psi(x_1, \cdots, x_m) = \phi_{ip}(x_1, \cdots, x_m).$$

Hence

$$\begin{aligned}\phi_{i1}(x_1, \cdots, x_m)\psi(\phi_{11}, \cdots, \phi_{m1}) &= \phi_{i,p+1}(x_1, \cdots, x_m)\\ &= \phi_{i1}(\phi_{1p}, \cdots, \phi_{mp})\\ &= \phi_{i1}[x_1\psi(x_1, \cdots, x_m), \cdots, x_m\psi(x_1, \cdots, x_m)]\\ &= \phi_{i1}(x_1, \cdots, x_m)\psi^n(x_1, \cdots, x_m),\end{aligned}$$

since $\phi_{i1}(x_1, \cdots, x_m)$ is a form of order n. We conclude that

$$\psi(\phi_{11}, \cdots, \phi_{m1}) = \psi^n(x_1, \cdots, x_m).$$

Hence $\psi(x_1, \cdots, x_m)$ is a solution of (1). *There exists a solution of* (1) *corresponding to any Cremona transformation of order n and finite period.*

The function ψ thus determined need not be the simplest solution of the functional equation for a given Cremona transformation : it may be factorable, and one of its factors may be a solution. For example, for the Cremona transformation

$$\begin{aligned}x' &= 3xyz - x^2w - 2y^3,\\ y' &= 2xz^2 - xyw - y^2z,\\ z' &= xyz - 2y^2w + yz^2,\\ w' &= xw^2 - 3yzw + 2z^3,\end{aligned}$$

of period 2, the function ψ is found to be

$$(x^2w^2 - 3y^2z^2 + 4xz^3 + 4wy^3 - 6xyzw)^2.$$

The square root of this function is transformed into its cube by the Cremona transformation, and we have Eisenstein's automorphism.

6. *Automorphisms of Determinants.* If the elements of a determinant $D \equiv |a_{ij}|$ of order n are independent variables, and A_{ij} is the cofactor of a_{ij}, the transformation $a'_{ij} = A_{ij}$ is a Cremona transformation of period 2, which transforms D into D^{n-1}.

Now suppose each element is a function of m variables, say

$$a_{ij} \equiv a_{ij}(x_1, \cdots, x_m),$$

and let

$$A_{ij} \equiv A_{ij}(x_1, \cdots, x_m).$$

In general, the equations

$$a_{ij}(x'_1, \cdots, x'_m) = A_{ij}(x_1, \cdots, x_m)$$

are inconsistent, and, when consistent, do not define $x'_1, \cdots, x'_m$ as rational integral functions of $x_1, \cdots, x_m$. In certain special cases we do obtain a transformation of the desired type.

Consider, for example, the symmetric determinant

$$\begin{vmatrix} a & d & e \\ d & b & f \\ e & f & c \end{vmatrix}.$$

The variables d, e, f occur twice, but their respective cofactors are the same in both cases. The determinant is transformed into its square by the transformation $a' = bc - f^2$, etc., each element being replaced by its cofactor. Eisenstein* credits this diophantine automorphism to Lagrange.

HARVARD UNIVERSITY

* Journal für Mathematik, vol. 27, p. 105.