SEPARABLE DIOPHANTINE EQUATIONS

BY

E. T. BELL

Theoretically, as noted by Skolem [3, p. 2](1), the general problem of algebraic diophantine analysis is reducible to the case in which occur only equations and inequalities of degree not higher than the second. For the extensive class of separable systems defined in §6, this reduction can be performed effectively, eventuating in the complete integer solutions of the equations concerned. The general method is strictly elementary, but none the less powerful within its natural range on that account. Among the more immediate applications are complete solutions of certain types of homogeneous equations of the second degree, only special cases of which have been solved hitherto by advanced methods, including that of generalized quaternions. The equation $x_1^2+\cdots+x_n^2=y^2$, for example, does not seem to be adapted to such methods, as a sum of n squares is not factorable, for all n, in a ring.

For simplicity of statement only, the method is presented for the domain of rational integers. A few slight and obvious verbal changes suffice to extend the entire discussion to any unique factorization domain, in particular to domains in which there is a Euclidean algorithm. The extension to principal ideal rings of algebraic integers, for instance, yields results of interest in the domain of rational integers.

I. Extended multiplicative equations

1. **Extended and simple systems.** With the exception of the symbol $\sum$ of summation, all letters throughout the paper denote rational integers.

A monomial $x^a y^b\cdots z^c$ in which $x, y, \cdots, z$ are independent variables (or independent unknowns), and $a, b, \cdots, c$ are constants greater than 0, is *elementary* if at least one of $a, b, \cdots, c$ is restricted to be 1 and $a+b+\cdots+c>1$.

Whether elementary or unrestricted, the monomials in a set are *independent* if no two of them have a variable in common.

An equation of the type

$$m_1X_1+\cdots+m_nX_n=0,$$

in which $n>2$, $m_1, \cdots, m_n$ are constants all different from zero, and $X_1, \cdots, X_n$ are independent elementary monomials, is an *extended multiplicative equation.*

Two extended multiplicative equations are *connected* if they have in com-

Presented to the Society, August 14, 1944; received by the editors April 20, 1944.

(1) Numbers in brackets refer to the references cited at the end of the paper.

mon at least one variable. If each pair of a set of equations is connected, the set is *connected.* A single extended multiplicative equation, or a connected set, is an *extended system.*

The most important detail implicit in the last definition is that all the monomials in an extended system are elementary.

A set of equations of the type

$$c_1Y_1 = c_2Y_2 = \cdots = c_sY_s,$$

in which $s \geqq 2$, $c_1, \cdots, c_s$ are constants all different from zero, and $Y_1, \cdots, Y_s$ are independent monomials, is a *simple multiplicative set.*

Two simple multiplicative sets are *connected* if they have in common at least one variable. If each pair of two or more sets is connected, or if there is but one set, the totality of sets constitute a *simple system.*

An extended system is thus more general than a simple system in that the equations of the extended system are not restricted, as in the simple system, to two terms. A simple system is more general than an extended system in that the monomials in the simple system are not restricted, as in the extended system, to be elementary.

In the method for extended systems developed here, the known theory of simple systems [1; 4] is a prerequisite. Acquaintance with algoristic details of that theory, however, is not necessary for following the applications to the solution of extended systems, as enough of the technique is recalled incidentally in the next four sections.

2. **Expansion and contraction.** The monomial $x^ay^b \cdots z^c$ is *expanded* with respect to any one of its variables $x, y, \cdots, z$, say z, if z^c is replaced by the product of c variables, say $z_1, \cdots, z_c$, all distinct from one another and from the remaining variables $x, y, \cdots$ in the given monomial. Thus the expansion with respect to z is $x^ay^b \cdots z_1 \cdots z_c$ with $x, y, \cdots, z_1, \cdots, z_c$ all distinct. The *total expansion*

$$x_1 \cdots x_a y_1 \cdots y_b \cdots z_1 \cdots z_c$$

is obtained by expanding with respect to each variable in turn. A totally expanded monomial of degree n is thus a product of first powers of n independent variables.

The inverse of expansion is contraction. A monomial is *contracted* with respect to any subset (proper or improper) of its variables by replacing each of the variables in the subset by the same variable, the new variable being distinct from all those not replaced. The *total contraction* is the result of replacing each of the variables in the monomial by the same variable. Thus the total contraction of $x^ay^b \cdots z^c$ is w^d, where $d = a+b+\cdots+c$.

In solving simple systems, at least one of the monomials in the system is totally expanded, and the system thus modified is solved. To the solution of the modified system are adjoined the equations giving the contractions neces-

sary to reproduce the original system. The modified system together with the equations of contraction constitute a new system. By repeated expansions and contractions the solution of the original system is obtained.

3. **Free and bound parameters.** A variable whose range of values is the integers is a *free parameter.*

Distinct variables $\xi, \eta, \cdots, \zeta$ which may take only such values as satisfy a *binding equation* of the form

$$m\xi^a\eta^b \cdots \zeta^c = n,$$

where $m, a, b, \cdots, c, n$ are constant integers and $mn \neq 0$, $a, b, \cdots, c > 0$, are *bound parameters.*

The solution of the indicated binding equation is equivalent to that of an *associated system* of linear diophantine equations. Let $p_1, \cdots, p_{[n]}$ be all the distinct positive prime divisors of n, and for any integer s, let $p_j^{s_j}$, $s_j \geqq 0$, be the highest power of p_j dividing s. By comparison of exponents of p_j in the binding equation, the associated linear system is

$$m_j + a\xi_j + b\eta_j + \cdots + c\zeta_j = n_j,$$
$$\xi_j \geqq 0, \eta_j \geqq 0, \cdots, \zeta_j \geqq 0, \qquad j = 1, \cdots, [n].$$

There are no solutions if the G.C.D. of $m_j, a, b, \cdots, c$ does not divide n_j (all j), or if for at least one j, $m_j > n_j$. If $|m| = 1$, and $\xi^a\eta^b \cdots \zeta^c$ is elementary, the system has solutions. If there are solutions, there are only a finite number, n', say

$$(\xi_j, \eta_j, \cdots, \zeta_j) = (\xi_{ji}, \eta_{ji}, \cdots, \zeta_{ji}), \qquad i = 1, \cdots, n'.$$

Let each of $e_\xi, e_\eta, \cdots, e_\zeta$ be a definite one of $1, -1$. All solutions of the binding equation are

$$(\xi, \eta, \cdots, \zeta) = (e_\xi p_j^{\xi_{ji}}, e_\eta p_j^{\eta_{ji}}, \cdots, e_\zeta p_j^{\zeta_{ji}}),$$

where the repeated index j indicates a product over $j = 1, \cdots, [n]$, and the units are assigned so that $e_\xi^a e_\eta^b \cdots e_\zeta^c = 1$ or -1 according as $mn > 0$ or $mn < 0$.

The detail of importance for extended systems is that the binding equation has solutions if $|m| = 1$ and $\xi^a\eta^b \cdots \zeta^c$ is elementary. The solution of a system of two or more binding equations is an immediate extension of the procedure for a single equation.

Binding equations arise as follows in solving either simple or extended systems. Constant coefficients $l, m, \cdots$ other than $1, -1$ are replaced by variables $\lambda, \mu, \cdots$ respectively, distinct among themselves and all distinct from the original variables in the system. Thus modified, the system has only unit coefficients. If a parametric solution of the modified system presents $\lambda, \mu, \cdots$ in the form $\lambda = l'L$, $\mu = m'M, \cdots$, where $l', m', \cdots$ are constants and $L, M, \cdots$ are monomials in the parameters, the binding equations are $l'L = l$, $m'M = m, \cdots$.

The concept of binding equations can be extended to equations of the type

$$m_1X_1 + \cdots + m_sX_s = n,$$

where $m_1, \cdots, m_s, n$ are constants not equal to 0, and $X_1, \cdots, X_s$ are monomials, not necessarily independent.

4. **Reducibility.** Each equation in a simple system has only two terms. An equation in more than two terms is *reducible* if it can be derived from a two-term equation by polynomial replacements of the variables in the two-term equation. A system of equations is *reducible* if each equation of the system in more than two terms is reducible. Unless otherwise noted, the coefficients in the substituted polynomials are restricted to be rational numbers, although this is not necessary; the discussion is almost the same if the coefficients are elements of the quotient field of any unique factorization domain.

Reducibility cuts across the order (number of terms) and the degree of equations and, where applicable, either provides a means of solving the equations or isolates their essential difficulties. It also unites apparently unrelated equations in classes according to the simple systems from which they are derivable, and makes possible a unified treatment of all.

5. **Examples for §4.** The arrow, $\rightarrow$, is to be read "is replaced by"; $(a, b, \cdots)$ denotes as usual the G.C.D. of $a, b, \cdots$. "Solution," as always, means "complete integer solution."

The solution of $\xi\eta = \zeta\phi$ is

$$\xi = ab, \qquad \eta = cd, \qquad \zeta = ad, \qquad \phi = cb,$$

a, b, c, d free parameters. If the parameters are restricted by the G.C.D. *condition* $(b, d) = 1$, the solution contains no duplications. The process of solving any simple system [1] automatically furnishes a set of G.C.D. conditions which, imposed, exclude duplications. These need not be stated if the objective, as here, is the solution.

Contraction with respect to ζ, ϕ adjoins the new equation $ad = bc$, of the same type as the original; whence there is the solution of

$$\xi\eta = \zeta^2:$$

$$\xi = fg^2, \qquad \eta = fh^2, \qquad \zeta = fgh, \qquad (g, h) = 1.$$

Of the infinity of equations reducible to the last, the following will suffice to illustrate reducibility:

$$x^2 + y^2 = z^2;$$

$$xy + yz + zx = 0;$$

$$x^2 + y^4 = z^2.$$

The first is derived by $\xi \rightarrow z+x$, $\eta \rightarrow z-x$, $\zeta \rightarrow y$. The solution is therefore given by $2x = f(g^2-h^2)$, $y = fgh$, $2z = f(g^2+h^2)$; whence the usual solution follows by considering the possible forms of f, g, h modulo 2. This equation is the total contraction of its total expansion

$$x_1x_2 + y_1y_2 = z_1z_2,$$

which is solvable. But for reasons which will appear in the discussion of separable equations, the solution of the totally contracted equation is not obtainable from that of its total expansion.

The second equation is derived by $\xi \to x+y$, $\eta \to x+z$, $\zeta \to x$; the solution is therefore

$$x = fgh, \qquad y = fg(g - h), \qquad z = fh(h - g).$$

The solution of the third equation is obtained from that of the second by applying the solution of the simple equation $fgh = k^2$: $f = c_1^2c_4c_5c_7c_9$, $g = c_2^2c_5c_6c_7c_8$, $h = c_3^2c_4c_6c_8c_9$, $k = c_1c_2c_3c_4c_5c_6c_7c_8c_9$, in 9 free parameters c_j.

It may be recalled that either of the methods [1; 4] for obtaining the solution of a simple system S produces the solution in terms of a certain number $N(S)$, characteristic of S, of parameters both necessary and sufficient for the solution. For $S \equiv fgh = k^2$, $N(S) = 9$, as above. For

$$S \equiv x^9 = y^5 = u^4v^4 = wrst,$$

all the variables being independent, $N(S) = 46, 217, 626$. Equally rudimentary systems for which $N(S)$ exceeds any preassigned number are readily constructed. Contraction increases $N(S)$. Thus for the totally expanded form S' of the last system, $N(S') = 1440$; and generally (a frequently occurring case), for

$$S \equiv x_1 \cdots x_a = y_1 \cdots y_b = \cdots = w_1 \cdots w_c,$$

the $a+b+ \cdots +c$ variables being independent, $N(S) = ab \cdots c$.

A point of some interest may be noted in passing. Geometrically, a simple system S defines a rational variety V in space of two or more dimensions, and V is parametrized by a certain number $n(V)$ of parameters. It is observed that $N(S)/n(V)$ tends to infinity more rapidly than any positive integral power of mvd, where m is the number of monomials, v the number of independent variables, and d is the highest degree of any monomial in S. It is not clear why specifying the integer points on V should so greatly increase the necessary and sufficient number of parameters. Libri [2] insisted that an algebraic diophantine system is "not indeterminate, $\cdots$, but overdetermined"; it is implicitly transcendental and should be extended by conditional equations (in circular functions) to exclude all but integer values of the variables. This proposal was rejected by Dirichlet as a valid but trivial heresy, and it has not been adopted. In any case it fails to yield the correct value for any $N(S)$.

To illustrate bound parameters,

$$mx^2 + ny^2 = nz^2,$$

with m, n constants not equal to 0, is derived from $\mu\xi^2 = \nu\eta\zeta$, in 5 variables,

whose solution is

$$\mu = gm_1m_2, \qquad \xi = n_1n_2n_3n_4n_5\theta\phi\psi,$$
$$\nu = gn_1n_2n_3n_4n_5^2, \qquad \eta = m_1n_1n_3\theta\phi^2, \qquad \zeta = m_2n_2n_4\theta\psi^2,$$

in 11 free parameters. The required solution is derived from this by

$$\mu \to m, \qquad \nu \to n, \qquad \xi \to x, \qquad \eta \to z + y, \qquad \zeta \to z - y,$$

so that now only θ, ϕ, ψ are free.

6. **Separability.** This concerns the sense in which "solution" is to be understood in the applications considered in later sections. The sense is a customary one; but for definiteness it is stated here in the form given by Skolem [2, p. 2]: "Im Falle unendlich vieler Lösungen sollen diese durch ein allgemeine Formel dargestellt werden, oder man soll ein Verfahren angeben, mit dessen Hilfe man alle Lösungen allmählich finden kann."

"Resolution" is used to avoid confusion between "solution" as "process of solving" and "solution" as "result of solving": a system is "resolved" to give its "solution." *Equivalent* resolutions are different processes of solving a system; they necessarily produce the same solution. The "Verfahren" is the resolution; the "Lösungen" the solution, meaning, as always, "complete solution." All resolutions of a given system are equivalent. It therefore suffices to produce one, if general formulas for the solution are not forthcoming.

A system S is *separable* if a resolution of S is equivalent to one or more of the following:

(A) the resolution of independent extended equations;

(B) the resolution of simple systems;

(C) the resolution of systems of linear diophantine equations, the total number of systems in (A), (B), (C) being finite.

It will be shown in the next section that there is a finite process for (A). Since finite processes are available for (B), (C), a separable system is resolvable and has a solution in the senses defined. It is to be noticed that the equations in (A) are independent. Some extended systems of more than one equation are separable, but not all such systems have been determined.

A possible connection between (A), (B), (C) is a source of further separable systems. Contraction of an extended equation with respect to some or all of its variables amounts to equating the values of these variables as given by the solution of the uncontracted equations. If the equations thus adjoined to the original equation are separable, the contracted equation is separable. In particular, if the adjoined equations are as in one or all of (A), (B), (C), the contracted equation is separable. A given extended equation when totally expanded thus generates a *class* of separable equations by contraction. At any stage of the process, binding equations may be imposed on some of the free parameters in the solution. The totality of equations in a class is determinable for a given extended equation. This classification cuts across the degree and

the number of independent variables in resolvable equations. For example, it will be seen that

$$x_1y_1z_1 + \cdots + x_ny_nz_n = 0,$$

in $3n$ independent variables x_j, y_j, z_j, and

$$m_1u_1^2 + \cdots + m_{n-1}u_{n-1}^2 = m_nv_1 \cdots v_s,$$

in $n+s-1$ independent variables u_i, v_j, with $m_1, \cdots, m_{n-1}$ arbitrary constants, are in the same class.

II. Applications

7. **Totally expanded type.** The totally expanded type of the general extended equation is

$$\sum_{i=1}^{n} m_i x_{i1} \cdots x_{is_i} = 0, \tag{7.1}$$

in which the m_i are constants not equal to 0, $n>2$, $s_i>1$, and the x_{ij} are $s_1+\cdots+s_n$ independent variables.

In solving (7.1), four further general types appear:

$$\xi_1\eta_1 + \cdots + \xi_n\eta_n = 0, \tag{7.2}$$

in which ξ_i, η_i, $i=1, \cdots, n$, are $2n$ independent variables;

$$\theta_1\phi_1 = \theta_2\phi_2 = \cdots = \theta_n\phi_n, \tag{7.3}$$

in $2n$ independent variables θ_i, ϕ_i;

$$uu_i = v_iw_i, \qquad i = 1, \cdots, n, \tag{7.4}$$

in which the u, u_i, v_i, w_i are $3n+1$ independent variables;

$$uu_i = m_iw_i, \qquad i = 1, \cdots, n, \tag{7.5}$$

in which the m_i are n constants not equal to 0, and the u, u_i, w_i are $2n+1$ independent variables. These four will be considered first.

The solution [3, p. 20 (13)] of (7.2) is

$$\xi_i = \alpha\alpha_i, \qquad \eta_i = -\sum_{j=1}^{j-1} \alpha_j\beta_{j,i} + \sum_{j=1}^{n-j} \alpha_{i+j}\beta_{i,i+j} \tag{7.6}$$

for $i=1, \cdots, n$, with the convention that a sum in which the lower limit exceeds the upper is vacuous. The $(n^2+n+2)/2$ parameters α, α_i, $\beta_{j,k}$ are free. If some of the signs in (7.5) are changed, the solution of the modified equation is obtained by making the corresponding changes in the values of either ξ_i or η_i in (7.6).

The resolution of (7.3) is recursive, the first step being the resolution of the $n-1$ equations

$$\theta_i\phi_i = \theta_n\phi_n, \qquad i = 1, \cdots, n-1.$$

The solution of the typical equation is

$$\theta_i = \lambda_{i1}\lambda_{i2}, \quad \phi_i = \lambda_{i3}\lambda_{i4}, \quad \theta_n = \lambda_{i1}\lambda_{i4}, \quad \phi_n = \lambda_{i3}\lambda_{i2},$$

in 4 free parameters λ_{ij}. In the second step the values of θ_n are equated, also those of ϕ_n. The resulting systems are of the general type (7.3) with $n-1$ in place of n. By repetitions of the process the solution of (7.3), involving $(n) \equiv 2^n$ free parameters $\lambda_1, \cdots, \lambda_{(n)}$, is obtained in the form

$$\theta_i = \Theta_i(\lambda_1, \cdots, \lambda_{(n)}), \quad \phi_i = \Phi_i(\lambda_1, \cdots, \lambda_{(n)}), \tag{7.7}$$

in which each of Θ_i, Φ_i is a monomial in $(n)/2$ of the parameters $\lambda_1, \cdots, \lambda_{(n)}$, each occurring only once in a particular Θ_i or Φ_i, and

$$\Theta_i(\lambda_1, \cdots, \lambda_{(n)})\Phi_i(\lambda_1, \cdots, \lambda_{(n)}) = \lambda_1 \cdots \lambda_{(n)},$$

for $i = 1, \cdots, n$.

The solution of the typical equation in (7.4) is

$$u = \theta_i\phi_i, \quad u_i = \psi_i\chi_i, \quad v_i = \theta_i\chi_i, \quad w_i = \psi_i\phi_i,$$

in 4 free parameters. The result of equating the values of u for $i = 1, \cdots, n$ is (7.3). The solution of (7.4) therefore follows from (7.7),

$$\begin{aligned} &u = \lambda_1 \cdots \lambda_{(n)}, && u_i = \psi_i\chi_i, \\ &v_i = \Theta_i(\lambda_1, \cdots, \lambda_{(n)})\chi_i, && w_i = \Phi_i(\lambda_1, \cdots, \lambda_{(n)})\psi_i, \end{aligned} \tag{7.8}$$

for $i = 1, \cdots, n$ in $2^n + 2n$ free parameters $\lambda_j, \psi_i, \chi_i$.

The solution of (7.5) is obtained from (7.8) by $v_i \to m_i$, so that now the χ_i and those of the λ_j occurring in the $\Theta_i(\lambda_1, \cdots, \lambda_{(n)})$, $i = 1, \cdots, n$, are bound parameters.

The resolution of (7.1) now follows from that of (7.2) by

$$m_i x_{i2} \cdots x_{is_i} \to \xi_i, \qquad x_{i1} \to \eta_i,$$

the first of which, by the first of (7.6), gives

$$\alpha\alpha_i = m_i x_{i2} \cdots x_{is_i}, \qquad i = 1, \cdots, n.$$

The resolution of this, by (7.5), (7.8), is reduced to that of the simple system

$$\begin{aligned} \Theta_i(\lambda_1, \cdots, \lambda_{(n)})\chi_i &= m_i, \\ x_{i2} \cdots x_{is_i} &= \Phi_i(\lambda_1, \cdots, \lambda_{(n)})\psi_i, \end{aligned} \tag{7.9}$$

for $i = 1, \cdots, n$. The first n equations in (7.9) are the binding equations from (7.5). The values of the $\lambda_j, \chi_i, \psi_i$ in the solution of (7.9) are substituted into

$$\alpha = \lambda_1 \cdots \lambda_{(n)}, \quad \alpha_i = \psi_i\chi_i; \tag{7.10}$$

and these values of α, α_i substituted into the second of (7.6) give

$$x_{i1} = -\sum_{j=1}^{n-1} \alpha_j \beta_{j,i} + \sum_{j=1}^{n-i} \alpha_{i+j} \beta_{i,i+j}. \tag{7.101}$$

The values of $x_{i2}, \cdots, x_{is_i}$ in the solution of the second of (7.9) and (7.101) give the solution of (7.1).

Explicit formulas for the monomials Θ_i, Φ_i can be given. They are complicated and will not be required. The second set of equations in (7.9) is solved first. The solution of the first equation, $i=1$, of the set gives the values of those of the $\lambda_1, \cdots, \lambda_{(n)}$ occurring in Φ_1 as monomials in new parameters, $\mu_1, \mu_2, \cdots$. These values are substituted into $\Phi_2, \cdots, \Phi_n$, and the second equation of the set then gives $\mu_1, \mu_2, \cdots$ as monomials in new parameters $\sigma_1, \sigma_2, \cdots$, and so on, till $i=n$. Finally the values of the λ's determined as monomials in all the parameters thus introduced are substituted into the binding equations in (7.9), which are solved as in §3.

8. **Contracted type.** The general contracted type derived from (7.1) is

$$\sum_{i=1}^{n} m_i X_{i1} \cdots X_{it_i} = 0, \tag{8.1}$$

in which $X_{i1}, \cdots, X_{it_i}$ is any contraction of $x_{i1}, \cdots, x_{is_i}$, so that the $X_{i1}, \cdots, X_{it_i}$, $i=1, \cdots, n$, are $t_1 + \cdots + t_n$ independent monomials. At least two subtypes of (8.1) are separable.

In the first, in at least one of the monomials in each product $X_{i1} \cdots X_{it_i}$, $i=1, \cdots, n$, at least one of the independent variables occurs only to the first power; say $X_{i1} = x_{i1} X'_{i1}$, where x_{i1}, X'_{i1} are independent. The equation is then

$$\sum_{i=1}^{n} m_i x_{i1} X'_{i1} X_{i2} \cdots X_{it_i} = 0, \tag{8.2}$$

which is the general extended multiplicative equation defined in §1. It is reduced to (7.2) by

$$m_i X'_{i1} X_{i2} \cdots X_{it_i} \to \xi_i, \qquad x_{i1} \to \eta_i,$$

and therefore, by (7.6), the associated simple system is

$$\alpha\alpha_i = X'_{i1} X_{i2} \cdots X_{it_i}, \qquad i = 1, \cdots, n. \tag{8.3}$$

The typical equation in (8.3) is of the general type

$$uv = w_1 \cdots w_t,$$

a simple equation whose solution may be given explicitly in terms of $2t$ free parameters. The resolution of (8.3) is then similar to that of (7.5), when the $X'_{i1}, X_{i2}, \cdots, X_{it_i}$ are regarded as independent variables. In the solution the $X'_{i1}, \cdots$ are replaced by their expressions as monomials in the independent variables x_{ij}. The result is a simple system in these variables.

A second separable type of (8.1) follows from the first on further contraction, but with respect to x_{i1} and another variable in the term in which x_{i1} occurs, for some or all of the terms in (8.2). The resolution of the equation thus contracted is reduced to that of the system of equations obtained from the solution of (8.2) by equating therein the values of the contracted variables. If the resulting system of equations is linear in some set of the free parameters in the solution of (8.2), the contracted equation is separable.

The cases of greatest interest are those in which the linear system has nontrivial solutions. If the linear system is s homogeneous equations in s unknowns, or if it is overconditioned, it gives merely a set of necessary conditions for the resolvability of the contracted equation. This is the case, for example, for homogeneous equations of the second degree derived from (7.1) with $s_i=2$, $i=1, \cdots, n$, by total contraction of each term.

9. **Equal sums of squares.** The solution of

$$\sum_{i=1}^{n} x_i^2 = \sum_{i=1}^{n} y_i^2 \tag{9.1}$$

is immediate from (7.2), (7.6) by

$$\xi_i \rightarrow x_i + y_i, \qquad \eta_i \rightarrow x_i - y_i:$$

$$\begin{aligned} 2x_i &= -\sum_{j=1}^{i-1} \alpha_j\beta_{j,i} + \alpha\alpha_i + \sum_{j=1}^{n-i} \alpha_{i+j}\beta_{i,i+j}, \\ 2y_i &= \sum_{j=1}^{i-1} \alpha_j\beta_{j,i} + \alpha\alpha_i - \sum_{j=1}^{n-i} \alpha_{i+j}\beta_{i,i+j}. \end{aligned} \tag{9.2}$$

By (9.1), (9.2) the resolution of

$$\sum_{i=1}^{n} x_i^2 = \sum_{i=1}^{n-1} y_i^2 \tag{9.3}$$

is reduced to that of

$$\sum_{j=1}^{n-1} \alpha_j\beta_{j,n} + \alpha\alpha_n = 0,$$

whose solution may be written down by a change of notation from (7.6). The solution of (9.3) then follows by substitution into (9.2).

Similarly, the resolution of

$$x_1^2 + x_2^2 + \cdots + x_n^2 = y^2 \tag{9.4}$$

is reduced to that of

$$\sum_{j=1}^{i-1} \beta_{j,i}\alpha_i + \alpha\alpha_i - \sum_{j=1}^{n-i} \beta_{i,i+j}\alpha_{i+j} = 0, \qquad i = 1, \cdots, n-1,$$

a system of $n-1$ homogeneous linear diophantine equations in n unknowns $\alpha, \alpha_1, \cdots, \alpha_{n-1}$. Hence (9.4) is separable.

Explicit formulas for the solution of (9.4) may be given. Let β_j be the determinant (of order $n-1$) obtained by deleting the jth column from the matrix ($n-1$ rows, n columns) of the system. The principal diagonal of β_n is $\alpha, \alpha, \cdots, \alpha$, and the determinant is skew symmetric about this diagonal. It follows from Cayley's diagonal expansion for a determinant of this type that $\alpha=0$ and $\beta_n=0$ are compatible only if all the elements of β_n vanish. This possibility is included as the trivial case $\rho=0$ in the solution below; otherwise, $\beta_n\neq 0$. Hence if ρ is any integer multiple of the reciprocal of the G.C.D. of $\beta_1, \cdots, \beta_n$,

$$\alpha_j = \rho(-1)^{j-1}\beta_j, \qquad j = 1, \cdots, n.$$

The solution of (9.4) is now written down from (9.2) by substituting these values of α_j into $x_1, \cdots, x_n$ and into $y_n \equiv y$.

From this solution that of

$$x_1^2 + \cdots + x_{n-1}^2 = uv \tag{9.5}$$

follows by $u \to y+x_n$, $v \to y-x_n$. More generally, as in solving (9.4), it is seen that

$$x_1^2 + \cdots + x_{n-s}^2 = u_1v_1 + \cdots + u_sv_s \tag{9.6}$$

is separable. By $u_j \to y_j+x_j$, $v_j \to y_j-x_j$, it follows that

$$x_1^2 + \cdots + x_n^2 = y_1^2 + \cdots + y_s^2 \tag{9.7}$$

is separable. But when $s \neq 1, n-1$, there are not explicit formulas for the solution.

10. **Equal sums of squares and elementary monomials.** The type

$$x_1^2 + \cdots + x_{n-s}^2 = u_1w_1 + \cdots + u_sw_s, \tag{10.1}$$

in which $x_1, \cdots, x_{n-s}, u_1, \cdots, u_s$ are n independent variables, $w_1, \cdots, w_s$ are s independent monomials in any number of variables, and all the variables in (10.1) are independent, is a generalization of (9.6). It is separable.

Each term on the left is first totally expanded, $x_i \to x_iy_i$, and the w_j are replaced by variables v_j so that the $2n$ variables in

$$x_1y_1 + \cdots + x_{n-s}y_{n-s} - v_1u_1 - \cdots - v_su_s = 0$$

are independent. By (7.6) the solution of this equation is

$$x_i = \alpha\alpha_i, \qquad y_i = -\sum_{j=1}^{i-1} \alpha_j\beta_{j,i} + \sum_{j=1}^{n-i} \alpha_{i+j}\beta_{i,i+j}, \qquad i = 1, \cdots, n-s;$$

$$v_k = \alpha\alpha_k, \qquad u_k = -\sum_{j=1}^{k-1} \alpha_j\beta_{j,k} + \sum_{j=1}^{n-k} \alpha_{k+j}\beta_{k,k+j}, \qquad k = 1, \cdots, s.$$

Contraction with respect to x_i, y_i,

$$(10.2) \qquad -\sum_{j=1}^{i-1} \alpha_j\beta_{j,i} - \alpha\alpha_i + \sum_{j=1}^{n-i} \alpha_{i+j}\beta_{i,i+j} = 0, \qquad i = 1, \cdots, n-s,$$

and the substitution

$$(10.3) \qquad \alpha\alpha_k = w_k, \qquad k = 1, \cdots, s,$$

reduce the resolution of (10.1) to that of the linear system (10.2) in $\alpha_1, \cdots, \alpha_n$ and the simple system (10.3). Hence (10.1) is separable. If $s=1$, explicit formulas for the solution may be given, as for (9.4), when (10.3) is solved explicitly for specific $w_1, \cdots, w_k$.

11. **Generalization of §§9, 10.** By $s_i=2$, $x_{i1}\rightarrow x_i$, $y_{i1}\rightarrow y_i$, (7.1) becomes

$$(11.1) \qquad m_1x_1y_1 + \cdots + m_nx_ny_n = 0,$$

with arbitrary integer coefficients m_i. The cases $m_i=1$, $i=1, \cdots, n$, and its contractions treated in §9 are included in (11.1), and their solutions can be obtained by properly specializing that of (11.1). But the argument for (9.4) is inapplicable to the corresponding step in the resolution of (11.1), as the elements in the principal diagonal of the determinant concerned are not necessarily all positive or all negative; and the greater simplicity of the special case, also its historical interest, justify the separate treatment in §9.

By $\xi_i\rightarrow u_iv_i$, $\eta_i\rightarrow w_i$, (7.2) becomes

$$u_1v_1w_1 + \cdots + u_nv_nw_n = 0,$$

and hence, from (7.6), for $i=1, \cdots, n$,

$$(11.2) \qquad \alpha\alpha_i = u_iv_i,$$

$$(11.3) \qquad w_i = -\sum_{j=1}^{i-1} \alpha_j\beta_{j,i} + \sum_{j=1}^{n-i} \alpha_{i+j}\beta_{i,i+j}.$$

The solution of (11.1) will follow from these by $u_i\rightarrow m_i$, $v_i\rightarrow x_i$, $w_i\rightarrow y_i$.

The solution of the typical equation (11.2) is written in the form

$$\alpha = a_ib_i, \qquad \alpha_i = c_i\pi_i, \qquad u_i = c_ia_i, \qquad v_i = b_i\pi_i.$$

Hence the a_i, b_i are given by the simple system

$$(11.4) \qquad (\alpha =)a_1b_1 = \cdots = a_nb_n,$$

which is of the type (7.3). The solution of (11.4) gives each of a_i, b_i as a monomial in 2^{n-1} distinct free parameters, and for each i the monomials a_i, b_i are independent.

With the a_i, b_i as determined by (11.4), the solution of (11.1) is thus

$$(11.5) \qquad x_i = b_i\pi_i, \qquad y_i = -\sum_{j=1}^{i-1} c_j\beta_{j,i}\pi_j + \sum_{j=1}^{n-i} c_{i+j}\beta_{i,i+j}\pi_{i+j},$$

with the binding equations

$$c_i a_i = m_i, \qquad i = 1, \cdots, n. \tag{11.6}$$

The free parameters are the π's and β's, in all $n(n+1)/2$, and there are 2^n+n bound parameters in the b_i, c_i determined by (11.4), (11.6).

The solution of

$$\sum_{i=1}^{n} m_i x_i^2 = \sum_{i=1}^{n} m_i y_i^2 \tag{11.7}$$

follows from $x_i \to x_i + y_i$, $y_i \to x_i - y_i$ applied to (11.5).

The solution of

$$\sum_{i=1}^{n} m_i x_i^2 = \sum_{i=1}^{n-1} m_i y_i^2 \tag{11.8}$$

is obtained from that of (11.7) by substituting the $\beta_{j,n}$, π_j determined by

$$\sum_{j=1}^{n-1} c_j \beta_{j,n} \pi_j = 0,$$

which is of the general type (11.1), into the solution of (11.7).

If $n=2$,

$$m_1 x_1^2 + \cdots + m_{n-1} x_{n-1}^2 + m_n x_n y_n = 0 \tag{11.9}$$

is a simple equation. Let $n>2$. The solution of (11.9) or, what is equivalent by $x_n \to x_n + y$, $y_n \to x_n - y$, that of

$$m_1 x_1^2 + \cdots + m_n x_n^2 = y^2 \tag{11.10}$$

falls into two parts. Contraction of (11.1) with respect to x_i, y_i, $i=1, \cdots, n-1$, gives (11.9), and hence, by (11.5),

$$-\sum_{j=1}^{i-1} c_j \beta_{j,i} \pi_j - b_i \pi_i + \sum_{j=1}^{n-i} c_{i+j} \beta_{i,i+j} \pi_{i+j} = 0, \qquad i = 1, \cdots, n-1, \tag{11.11}$$

a system of $n-1$ linear homogeneous equations in $\pi_1, \cdots, \pi_n$.

If the values assigned to the β's (which are free parameters) are such that not all determinants of order $n-1$ in the matrix of the system (11.11) vanish, the β's and the system are *regular*, in the contrary case, *singular*, and likewise for the corresponding solutions.

In the regular case let m be an arbitrary integer multiple of the reciprocal of the G.C.D. (for specific β's) of the n determinants of order $n-1$ in the matrix, and let β_i be the determinant obtained by deleting the ith column of the matrix. Then

$$\pi_i = (-1)^{i-1} m \beta_i, \qquad i = 1, \cdots, n;$$

and by (11.5) the regular solution of (11.9) is

$$x_i = (-1)^{i-1} m b_i \beta_i, \qquad i = 1, \cdots, n,$$

$$y_n = -m \sum_{j=1}^{n-1} (-1)^{j-1} c_j \beta_j \beta_{j,n}. \tag{11.12}$$

In the singular case, let $\theta_1, \cdots, \theta_n$ be integer parameters, restricted for the moment so that the vector $(\theta_1, \cdots, \theta_n)$ is not equal to any row vector of the matrix of (11.11) in the singular case. Then the determinant of the system formed by adjoining

$$\theta_1 \pi_1 + \cdots + \theta_n \pi_n = 0 \tag{11.13}$$

to (11.11) vanishes, and hence the augmented system has a non-trivial solution. Let m' be any integral multiple of the reciprocal of the G.C.D. of the determinants β_i' of the matrix of the system formed by (11.13) (as the first equation) and the $n-1$ equations obtained by omitting the last equation in (11.11). Then

$$\pi_i = (-1)^{i-1} m' \beta_i', \qquad i = 1, \cdots, n,$$

and the singular solution is written down from (11.12) by the change in notation $m \to m'$, $\beta_i \to \beta_i'$. The restriction on $(\theta_1, \cdots, \theta_n)$ may be removed, as it excludes only the trivial solution, so that $\theta_1, \cdots, \theta_n$ in the singular solution are n distinct free parameters.

The discussion for

$$a_1 x_1^2 + \cdots + a_n x_n^2 = b_1 y_1^2 + \cdots + b_s y_s^2 \tag{11.14}$$

parallels that of (9.7), and may be omitted. Likewise for (10.1) and

$$a_1 x_1^2 + \cdots + a_{n-s} x_{n-s}^2 = b_1 u_1 w_1 + \cdots + b_s u_s w_s, \tag{11.15}$$

with the a's, b's arbitrary constants and the rest of the notation as in (10.1).

By the classical rational reduction of the general quadratic form $Q(x_1, \cdots, x_t)$ with integer coefficients to a sum of squares with rational number coefficients, it follows from (11.15) that

$$Q(x_1, \cdots, x_{n-s}) = b_1 u_1 w_1 + \cdots + b_s u_s w_s \tag{11.16}$$

is separable. This includes all the preceding results (and an infinity more).

For general n the equations in §§7–11 are irreducible, as reducibility is defined in §4. They are also irreducible in the usual sense in any ring.

12. **Example for §11.** The unavoidable calculations for a given n are concentrated in (11.4). It will be sufficient to indicate the details for $n=3$. In that case (11.1) is

$$m_1 x_1 y_1 + m_2 x_2 y_2 + m_3 x_3 y_3 = 0,$$

and the corresponding solution of (11.4) is

$$a_1 = \gamma_1\gamma_2\delta_3\delta_4, \quad a_2 = \gamma_1\gamma_4\delta_2\delta_3, \quad a_3 = \gamma_1\gamma_2\gamma_3\gamma_4,$$
$$b_1 = \gamma_3\gamma_4\delta_1\delta_2, \quad b_2 = \gamma_2\gamma_3\delta_1\delta_4, \quad b_3 = \delta_1\delta_2\delta_3\delta_4.$$

From the general discussion, the solution is

$$x_1 = b_1\pi_1, \quad y_1 = c_2\beta_{1,2}\pi_2 + c_3\beta_{1,3}\pi_3,$$
$$x_2 = b_2\pi_2, \quad y_2 = -c_1\beta_{1,2}\pi_1 + c_3\beta_{2,3}\pi_3,$$
$$x_3 = b_3\pi_3, \quad y_3 = -c_1\beta_{1,3}\pi_1 - c_2\beta_{2,3}\pi_2,$$

with the binding equations

$$m_1 = c_1a_1, \quad m_2 = c_2a_2, \quad m_3 = c_3a_3.$$

By §3 the binding equations have solutions and are resolvable for any given m_1, m_2, m_3.

From the above solution those of the several contractions of the original equation are readily obtained by following the directions for the general case. As pointed out, the solution of the totally contracted equation

$$m_1x_1^2 + m_2x_2^2 + m_3x_3^2 = 0$$

is not obtainable by this method. The equations of total contraction will have non-trivial solutions π_1, π_2, π_3 if and only if

$$b_1c_2c_3\beta_{2,3}^2 + b_2c_1c_3\beta_{1,3}^2 + b_3c_1c_2\beta_{1,2}^2 = -b_1b_2b_3$$

has solutions $\beta_{2,3}, \beta_{1,3}, \beta_{1,2}$, or, what is equivalent, if and only if $-\alpha^2$, where $\alpha \equiv \gamma_1\gamma_2\gamma_3\gamma_4\delta_1\delta_2\delta_3\delta_4$, is represented in the form

$$m_1m_2\beta_{1,2}^2 + m_2m_3\beta_{2,3}^2 + m_1m_3\beta_{1,3}^2.$$

When this condition is satisfied, the solutions of the totally contracted equation are found from those of the totally expanded equation by substituting therein the values of π_1, π_2, π_3 determined by

$$-b_1\pi_1 + c_2\beta_{1,2}\pi_2 + c_3\beta_{1,3}\pi_3 = 0,$$
$$-c_1\beta_{1,2}\pi_1 - b_2\pi_2 + c_3\beta_{2,3}\pi_3 = 0,$$

for each set of values of $\beta_{1,2}, \beta_{2,3}, \beta_{1,3}$ representing $-\alpha^2$ in the above form.

On another occasion examples of separable equations and separable systems of higher degrees will be given. An example of a separable equation whose solution is immediate from the calculations of this section is

$$axy + bzw = cu^3,$$

a, b, c arbitrary constants.

References

1. E. T. Bell, *Reciprocal arrays and diophantine analysis*, Amer. J. Math. vol. 55 (1933) pp. 50–66.

2. G. Libri, *Exposition d'un principe générale qui renferme toute la théorie des nombres.* Memorie della Reale Accademia della Scienze di Torino vol. 28 (1824) pp. 272–280; also, ibid. p. 254. The "general principle" was extensively applied in several later papers; this was its first appearance.

3. Th. Skolem, *Diophantische Gleichungen*, Ergebnisse der Mathematik und ihrer Grenzgebiete vol. 5 (1938) no. 4.

4. M. Ward, *A type of multiplicative diophantine systems*, Amer. J. Math. vol. 55 (1933) pp. 67–76. The large $N(S)$ in §5 is from this paper, where $N(S)$ is determined for certain types of S.

California Institute of Technology