# POLYNOMIAL DIOPHANTINE SYSTEMS*

BY

E. T. BELL

1. Formal definitions of polynomial diophantine systems, as understood in this paper, are given in §5, after the necessary algebraic preliminaries in §2 and certain arithmetical considerations in §4. The algebraic structure of the systems is stated in §3. Roughly, the systems are of the following type.

*As always henceforth, let n denote an arbitrary constant (finite) integer* $>1$. Let $a, b, \cdots, c$ be $mn$ ($m$ finite, $\geqq 1$) integers $>0$, and let $P_\alpha, Q_\beta, \cdots, R_\gamma$ ($\alpha=1, \cdots, a$; $\beta=1, \cdots, b$; $\cdots$; $\gamma=1, \cdots, c$) be polynomials in $sn$ independent variables $x_1, \cdots, x_{sn}$ ($s$ finite, $\geqq 1$) with integer (not necessarily rational integer) coefficients. Let the system $\Sigma$,

$$\Sigma: P_1 = \cdots = P_a, Q_1 = \cdots = Q_b, \cdots, R_1 = \cdots = R_c,$$

be consistent and indeterminate.

The systems $\Sigma$ considered have an infinity of integer solutions, all of which can be given explicitly by expressing $x_1, \cdots, x_{sn}$ as polynomials in parameters ranging over all integers, with integer coefficients, and for this complete solution only an application of the fundamental theorem of arithmetic (unique prime decomposition) is necessary. Homogeneous and inhomogeneous systems $\Sigma$ are treated by the same analysis, and the degrees of the polynomials are unrestricted. The simple algorithm for obtaining the complete solution in integers is indicated in §7, with examples.†

The remarkable features are the complete, explicit, solvability and the intimate connection with the fundamental theorem. In these respects systems $\Sigma$ are an immediate generalization in one direction of the Pythagorean equation $x^2+y^2=z^2$ and its complete solution in rational integers. Naturally, the polynomials composing a system $\Sigma$ can not be given arbitrarily; applicability of the fundamental theorem imposes necessary restrictions. We proceed to the algebra sufficient for the construction of general systems $\Sigma$.

2. Let $R$ be an abstract commutative ring in which the identities with respect to addition, multiplication are $z$, $u$ respectively, and in which the sum, product of any elements $a$, $b$ in $R$ are written $a+b$, $ab$ respectively.

---

* Presented to the Society, October 28, 1933; received by the editors May 26, 1933.

† In all of the examples constructed (only 3 are reproduced here) all of the polynomials in the systems are irreducible in the ring of their values, but I can not prove that all polynomials in the most general system constructed are irreducible.

Since $R$ may contain nilfactors, $ax=bx$, $x\neq z$ do not necessarily imply $a=b$. In the special case when $R$ is a domain of integrity, the cancellation law holds. Conversely, in the special case when cancellation holds, $R$ is a domain of integrity. For if $p\neq z, q\neq z, pq=z$, then $pq=pz$, and hence $q=z$, a contradiction. Unless so stated it is not assumed that $R$ (or any other commutative ring) is a domain of integrity.

The elements of $R$ will be called *integers*; to avoid confusion, $0, \pm 1, \pm 2, \cdots$ will always be characterized as rational integers.

Integers other than $z$, $u$ will frequently be indicated by a multiple index notation, $x(i, j)$, $y(k, t)$, $x(i_1, \cdots, i_s; j)$, the $i, j, k, t$ being the indices. In a symbol with precisely 2 indices, say $x(i, j)$, the first index $(i)$ ranges over all rational integers $>0$, the second $(j)$ ranges over only $1, \cdots, n$.

A symbol with precisely 1 index, say $x(i)$, denotes a *vector* (one-rowed matrix) of $n$ integers,

$$x(i) = (x(i, 1), \cdots, x(i, n));$$

the $j$th *coordinate* of $x(i)$ is $x(i, j)$. Vectors being matrices, vector equality, $x(i)=y(k)$, is matrix equality, $x(i, j)=y(k, j)$ $(j=1, \cdots, n)$.

It is postulated that there exists in $R$ a set $\phi$ of integers $\phi(i, j, k)$ $(i, j, k=1, \cdots, n)$ such that

$$\phi(1, s, k) = \delta_{sk} \qquad (s, k = 1, \cdots, n) \tag{2.1}$$

$$[\delta_{ss} = u, \delta_{sk} = z, s \neq k];$$

$$\phi(i, j, k) = \phi(j, i, k) \qquad (i, j, k = 1, \cdots, n); \tag{2.2}$$

$$\sum_{j=1}^{n}\phi(p, q, j)\phi(j, r, t) = \sum_{j=1}^{n}\phi(p, r, j)\phi(j, q, t) \quad (p, q, r, t = 1, \cdots, n). \tag{2.3}$$

Let $c_{pj}(p, j=1, \cdots, n)$ be integers, such that $c_{1j}=\delta_{1j}$ $(j=1, \cdots, n)$ and the determinant $|c_{pj}|$ ($p$ row, $j$ column) of the matrix $\|c_{pj}\|$ has the value $u$. Let $c'_{pj}$ denote the cofactor of $c_{pj}$ in $|c_{pj}|$. Then $c'_{pj}=u$, and

$$\sum_{j=1}^{n}c_{pj}c'_{rj} = \delta_{pr} = \sum_{j=1}^{n}c_{jp}c'_{jr} \qquad (p, r = 1, \cdots, n).$$

Define the set $\phi'$ of integers $\phi'(r, s, t)$ $(r, s, t=1, \cdots, n)$ by

$$\phi'(r, s, t) \equiv \sum_{j,k,h=1}^{n} c_{rj}c_{sk}c'_{th}\phi(j, k, h).$$

Then it is easily seen (by manipulation of dummy suffixes as in tensor algebra) that

$$\phi(r, s, t) = \sum_{j,k,h=1}^{n} c'_{jr}c'_{ks}c_{ht}\phi'(j, k, h).$$

Similarly, and by using (2.1)–(2.3), we see that the $\phi'(r, s, t)$ satisfy the same relations: the symbol $\phi$ in (2.1)–(2.3) can be replaced by $\phi'$. We shall say that the sets $\phi$, $\phi'$ are *equivalent*, $\phi \sim \phi'$. The relation of equivalence is reflexive ($\phi \sim \phi$), symmetric (if $\phi \sim \phi'$ then $\phi' \sim \phi$), and transitive (if $\phi \sim \phi'$ and $\phi' \sim \phi''$, then $\phi \sim \phi''$). The consistency of (2.1)–(2.3) need not be discussed, as instances of $\phi$ will be evident when diophantine systems are constructed.

The $j$th coordinate, denoted by $x(i_a, i_b; j)$, in the *product* $x(i_a)x(i_b)$ of any vectors $x(i_a)$, $x(i_b)$, *to the base* $\phi$, is defined by

$$x(i_a, i_b; j) = \sum_{i_a, i_b=1}^{n} \phi(j_a, j_b; j)x(i_a, j_a)x(i_b, j_b) \quad (j = 1, \cdots, n). \tag{2.4}$$

In a given context the same base $\phi$ is presupposed. All equations persist if $\phi$ be replaced by $\phi'$, where $\phi \sim \phi'$.

The notation $u(i)(=u(k), \cdots)$ is reserved for the vector defined by $u(i, j) = \delta_{ij} (j = 1, \cdots, n)$. Hence, by (2.1), (2.4) we have

$$u(i)x(k) = x(k) \tag{2.5}$$

for all $x(k)$. If possible, let $v(i)x(k) = x(k)$, $v(i) \neq u(i)$, all $x(k)$. Choosing $x(k) = u(k)$, and referring to (2.5), we have the contradiction $v(i) = u(i)$. Hence $u(i)$ is the unique identity of vector multiplication.

The notation $z(i)(=z(k), \cdots)$ is reserved for the vector defined by $z(i, j) = z(j = 1, \cdots, n)$; $z(i)x(k) = z(i)$ for all $x(k)$.

The *sum* $x(i_a) + x(i_b)$ is the vector whose $j$th coordinate is the sum (in $R$) of the $j$th coordinates of $x(i_a)$, $x(i_b)$ $(j = 1, \cdots, n)$. Since $z$ is the unique identity of addition in $R$, $z(i)$ is the unique identity of vector addition.

There can be no confusion between operations in $R$ and the corresponding operations on vectors, since the notation for the operands indicates the species.

Now (2.2), (2.3) are necessary and sufficient conditions for commutativity and associativity of multiplication in any linear algebra with $n$ basal units, and (2.1) is a necessary and sufficient condition for the existence of an identity with respect to multiplication in the algebra. Since any commutative, associative linear algebra with an identity of multiplication has a vector representation with vector multiplication and addition as above defined, it follows that *the set, $VR$, of all vectors is a commutative ring, in which the identities of multiplication, addition are $u(i)$, $z(i)$ respectively.*

The notation $\epsilon(i)$, $\epsilon(k)$, $\cdots$ will be reserved for units in $VR$, which are defined as follows, and which are not to be confused with the usual unit vectors of linear algebra. If $\epsilon(i_1)$ is in $VR$, and if $\epsilon(i_2)$ exists in $VR$ such that

$$\epsilon(i_1)\epsilon(i_2) = u(i),$$

$\epsilon(i_1)$ is a *unit* in $VR$, and $\epsilon(i_2)$ is its *conjugate*. Hence the conjugate of a unit is a unit. Since $u(i)$ is its own conjugate, units exist. If possible, let $\epsilon(i) = z(i)$. Then $\epsilon(i)\epsilon'(i) = z(i)\epsilon'(i)$, where $\epsilon'(i)$ is the conjugate of $\epsilon(i)$. Hence the contradiction (in $R$) $u = z$. Thus no unit is equal to the zero in $VR$.

Suppose for a moment that $VR$ is a domain of integrity. If possible, let

$$\epsilon(i_1)\epsilon(i_2) = u(i) = \epsilon(i_1)\epsilon(i_3),\ \epsilon(i_2) \neq \epsilon(i_3).$$

Then $\epsilon(i_1)[\epsilon(i_2) - \epsilon(i_3)] = z(i)$. With $\epsilon(i_1) \neq z(i)$ this gives the contradiction $\epsilon(i_2) = \epsilon(i_3)$. Hence, if $VR$ is a domain of integrity, the conjugate of a given unit is unique.

We return to the general $VR$. In order that $\epsilon(i_1)$, $\epsilon(i_2)$ be conjugate units it is necessary and sufficient that

$$\sum_{r,s=1}^{n} \phi(r, s, j)\epsilon(i_1, r)\epsilon(i_2, s) = \delta_{1j} \qquad (j = 1, \cdots, n).$$

Let $a(i)$, $\alpha(i)$, $b(i)$, $\beta(i)$, $\xi(i)$ be such that

$$a(i) = \alpha(i)\xi(i),\ b(i) = \beta(i)\xi(i).$$

If $a(i)$, $b(i)$ are given, a solution of these equations is of the type

$$\alpha(i) = a(i)\epsilon(i),\ \beta(i) = b(i)\epsilon(i),\ \xi(i) = \epsilon'(i),$$

where $\epsilon(i)$, $\epsilon'(i)$ are arbitrary conjugate units. If this type exhausts the solutions, $a(i)$, $b(i)$ are said to be *coprime* (in $VR$). Necessary and sufficient conditions that $a(i)$, $b(i)$ be coprime are that the system

$$\begin{aligned}
&\sum_{r,s=1}^{n} \phi(r, s, j)\alpha(i, r)\xi(i, s) = a(i, j), \\
&\sum_{r,s=1}^{n} \phi(r, s, j)\beta(i, r)\xi(i, s) = b(i, j), \\
&\sum_{r,s=1}^{n} \phi(r, s, j)\xi'(i, r)\xi(i, s) = \delta_{1j} \qquad (j = 1, \cdots, n)
\end{aligned} \tag{2.6}$$

be solvable in $R$ for

$$\alpha(i, r),\ \beta(i, r),\ \xi(i, s),\ \xi'(i, r) \qquad (r, s = 1, \cdots, n).$$

3. Let $x(1), \cdots, x(s)$ be any vectors, and let $s > 2$. The $j$th coordinate in the product $x(1) \cdots x(s)$ will be denoted by $x(1, \cdots, s; j)$. By mathematical induction from (2.4) we find for $x(1, \cdots, s; j)$ the following explicit polynomial expression in $R$:

$$\sum \phi(j_1, j_2, k_1)\phi(k_1, j_3, k_2) \cdots \phi(k_{s-3}, j_{s-1}, k_{s-2})\phi(k_{s-2}, j_s, j)$$
$$\times x(1, j_1)x(2, j_2) \cdots x(s, j_s) \quad (j_1, \cdots, j_s, k_1, \cdots, k_{s-2} = 1, \cdots, n).$$

When $x(i) = x(i_1) = \cdots = x(i_t)(t>1)$ the product $x(i_1) \cdots x(i_t)$ is written $x^t(i)$, and its $j$th coordinate $x(i^{(t)}; j)$. Hence, the case $t=2$, $s_1=s_2=1$, included, we have defined $x^{s_1}(i_1) \cdots x^{s_t}(i_t)$ and its $j$th coordinate $x(i_1^{(s_1)}, \cdots, i_t^{(s_t)}; j)$.

If the $n$ coordinates of $x(i)$ are independent variables in $R$, $x(i)$ is called a *variable* (vector) in $VR$. The variables $x(i_1), \cdots, x(i_t)$ in $VR$ are said to be *independent* if their $nt$ coordinates are $nt$ independent variables in $R$. Denote the power product $x^{s_1}(i_1) \cdots x^{s_t}(i_t)$, where $s_1, \cdots, s_t$ are rational integers $>0$, of $t$ independent variables $x(i_1), \cdots, x(i_t)$ in $VR$ by $X(t)$, with a similar notation for any product of positive integral powers of independent variables in $VR$. The $r$ power products $X_1(t_1), \cdots, X_r(t_r)$ $(r>1)$ in $VR$ are said to be *independent* if all the variables in $VR$ composing these $r$ products are independent in $VR$.

Denote the $j$th coordinate of $X_i(t_i)$ by $X_i(t_i; j)$, and let $X_1(t_1), \cdots, X_r(t_r)$ be independent. Then the equations

$$X_1(t_1) = \cdots = X_r(t_r) \tag{3.1}$$

in $VR$ are equivalent to the simultaneous system

$$X_1(t_1; j) = \cdots = X_r(t_r; j) \qquad (j = 1, \cdots, n) \tag{3.2}$$

in $R$, as each of (3.1), (3.2) implies the other. With $a, b, \cdots, c, m$ as in §1, we pass to the general case. The power products in each row of

$$\begin{aligned} X_1(p_1) &= \cdots = X_a(p_a), \\ Y_1(q_1) &= \cdots = Y_b(q_b), \\ &\cdots \qquad\qquad \cdots \\ Z_1(r_1) &= \cdots = Z_c(q_c) \end{aligned} \tag{3.3}$$

are independent; in any pair of rows, at least one product in one of the rows and one product in the other are not independent; the system (3.3) does not separate into two or more systems with the two preceding characteristics in sets of independent variables in $VR$ having no variable in common. The set

$$\begin{aligned} X_1(p_1; j) &= \cdots = X_a(p_a; j), \\ Y_1(q_1; j) &= \cdots = Y_b(q_b; j), \\ &\cdots \qquad\qquad \cdots \\ Z_1(r_1; j) &= \cdots = Z_c(r_c; j) \qquad (j = 1, \cdots, n) \end{aligned} \tag{3.4}$$

in $R$, equivalent to (3.3) in $VR$, will be called a *polynomial system.*

If the complete solution in integers of a polynomial system is obtainable in explicit form in terms of polynomials in integer parameters with integer coefficients, we shall say the system is *diophantine.*

It will be seen that a sufficient condition that a polynomial system in $R$ be diophantine is that the fundamental theorem of arithmetic shall hold in $VR$. A generalization of (3.4) including arbitrary constant coefficients is noted in §7.

4. Unique decomposition is understood here in the strict sense, as in rational arithmetic or in the theory of ideals in an algebraic number field. For precision the postulates are stated. The notation in this section is independent of that in the rest of the paper.

Let $\Omega$ denote a set of at least two distinct elements $a, b, \cdots$, for which the postulates (4.1)–(4.7) hold.

(4.1) Equality is significant in $\Omega$; $a=b$ or $a\neq b$; equality is symmetric, reflexive, and transitive.

(4.2) There exists a binary operation which can be applied to any pair $a, b$ of elements of $\Omega$, in this order, to produce a unique element, denoted by $ab$, in $\Omega$.

(4.3) $ab=ba$; $a(bc)=(ab)c$, for all $a, b, c$ in $\Omega$.

(4.4) If $\Omega$ contains $z$ such that $zx=z$ for all $x$ in $\Omega$, $z$ is unique.

(4.5) If $\Omega$ contains $u$ such that $ux=x$ for all $x$ in $\Omega$, $u$ is unique, and $u\neq z$.

(4.6) If $\Omega$ contains the $z$ in (4.4), and $ab=z$, then $a=z$ or $b=z$ (or both).

(4.7) If $ax=bx$, $x\neq z$ (if $\Omega$ contains $z$), then $a=b$; if $\Omega$ does not contain $z$, then $ax=bx$ implies $a=b$.

We need not discuss the independence of (4.1)–(4.7). The consistency is obvious from numerous instances. Note that only one binary operation is postulated.

If $p, q, r$ are any elements $\neq z$ of $\Omega$ such that $p=qr$, we say that $r$ *divides* $p$, and write $r\,|\,p$ (hence also $q\,|\,p$). In all questions of divisibility $z$ is henceforth excluded.

If $u$ as in (4.5) exists, and $\epsilon\,|\,u$, $\epsilon$ in $\Omega$, $\epsilon$ is a *unit.* Hence $u=\epsilon\epsilon'$, and $\epsilon'$ is a unit; $\epsilon$, $\epsilon'$ are *conjugate* units. Obviously $u$ is a unit. If $\epsilon_1, \cdots, \epsilon_r$ are units, and $\epsilon_1', \cdots, \epsilon_r'$ their respective conjugates, $\epsilon_1 \cdots \epsilon_r$ and $\epsilon_1' \cdots \epsilon_r'$ are conjugate units. From (4.5), (4.7), a unit has a unique conjugate. If $x\,|\,a$ and $x\,|\,b$ imply that $x$ is a unit, $a, b$ are *coprime.* If $a\,|\,b$ and $b\,|\,a$, $a, b$ are *associates,* $a\sim b$. From $a\sim b$ follows $a=\epsilon b$, $\epsilon$ unit.

An element $h$ in $\Omega$ other than a unit such that $x\,|\,h$ only when $x\sim h$ or a unit, is *irreducible.* An irreducible element $p$ is *prime* if $p\,|\,ab$ implies at least one of $p\,|\,a$, $p\,|\,b$. (This amounts to making all irreducibles primes—not the case in general in an algebraic integer ring.)

If $d \mid a$ and $d \mid b$ imply $d \mid g$, $g \mid a$, $g \mid b$, $g$ is the G.C.D (by definition) of $a$, $b$.

We define $\Omega$ to be an *arithmetic* with respect to the binary operation in (4.2), and write $A\,\Omega$, if the postulates (4.8), (4.9) hold.

(4.8) If $b$ is any element of $\Omega$, there exist only a finite number of elements $x_i$ of $\Omega$ different from units such that $x_i \mid b$.

(4.9) Apart from permutations of $\epsilon$, $p_1, \cdots, p_r$, every element $b$ of $\Omega$ is uniquely expressible in the form $b = \epsilon p_1 \cdots p_r$, where $\epsilon$ is a unit and $p_1, \cdots, p_r$ are primes.

Rational arithmetic and the theory of algebraic numbers and ideals provide several instances of $A\,\Omega$. We have not attempted to state a minimum set of postulates sufficient for unique factorization, as we are concerned here only with the application to be made presently of the fundamental theorem to diophantine analysis. In particular, (4.9) is a consequence of the rest, which can be weakened. An exhaustive study of postulate systems leading to (4.9) has been made by Professor M. Ward in an unpublished paper.

The following consequence of the postulates will be required. If $a \mid bc$, and $a$, $b$ are coprime, then $a \mid c$. For, the hypotheses are equivalent to $ad = bc$, with $a$, $b$ coprime. Let $p \mid a$, where $p$ is prime. Then $p \mid b$ or $p \mid c$. But $p \mid b$ is impossible.

5. We return to polynomial systems as defined in §3. A polynomial system will be characterized as diophantine if all integer values of the independent variables satisfying the system can be given explicitly by expressing the variables as polynomials with integer coefficients in a finite number of independent parameters ranging independently over all integers.

It will now be shown that any instance, say $AVR$, of $VR$ which is an arithmetic in the sense of §4 with respect to vector multiplication as in §2 provides an infinity of polynomial diophantine systems.

The system (3.3) is purely multiplicative. Hence, since we are now operating in $AVR$, the method of reciprocal arrays developed in a previous paper* can be applied to obtain the complete solution of (3.3) in parametric form. The solution expresses each of the independent variables (elements of $AVR$) as power products of parameters in $AVR$. The method of arrays is applicable because it refers to any arithmetic as defined in §4. For clearness we illustrate the process by giving the first step in the proof, from which (as in the paper cited) the rest follows by mathematical induction, in the form adapted to the present discussion.

---

* American Journal of Mathematics, vol. 55 (1933), pp. 50–66.

For simplicity, let Greek letters denote elements of $AVR$ for the moment. We shall find all $\alpha, \beta, \gamma, \delta$ such that

$$\alpha\beta = \gamma\delta.$$

Denote the G.C.D. of $\alpha, \gamma$ by $\sigma$. Then $\alpha = \sigma\alpha_1$, $\gamma = \sigma\gamma_1$, where $\alpha_1, \gamma_1$ are coprime. Hence $\alpha_1\beta = \gamma_1\delta$, and therefore (by the definition of divisibility and the last of §4) $\alpha_1 \mid \delta$ and $\gamma_1 \mid \beta$. Thus $\delta = \alpha_1\delta_1$, $\beta = \gamma_1\beta_1$. With the given equation this yields $\beta_1 = \delta_1$. Denote the common value of $\beta_1, \delta_1$ by $\tau$. Then the complete solution is

$$\alpha = \alpha_1\sigma, \beta = \gamma_1\tau, \gamma = \gamma_1\sigma, \delta = \alpha_1\tau.$$

Moreover, it is sufficient to choose only such values of the parameters as are coprime.*

Consider now (3.3). The independent variables, say $\xi, \eta, \cdots, \zeta$, are in $AVR$. Let the $\rho, \sigma, \cdots, \tau$ be parameters ranging independently over all the elements of $AVR$. The method of reciprocal arrays gives the complete solution of (3.3) in the form

$$\begin{aligned}
\xi &= \rho_1^{a_1} \cdots \rho_r^{a_r} \sigma_1^{b_1} \cdots \sigma_s^{b_s} \cdots \tau_1^{c_1} \cdots \tau_t^{c_t}, \\
\eta &= \rho_1^{f_1} \cdots \rho_r^{f_r} \sigma_1^{g_1} \cdots \sigma_s^{g_s} \cdots \tau_1^{h_1} \cdots \tau_t^{h_t}, \\
&\cdots \qquad \cdots \qquad \cdots \\
\zeta &= \rho_1^{k_1} \cdots \rho_r^{k_r} \sigma_1^{l_1} \cdots \sigma_s^{l_s} \cdots \tau_1^{m_1} \cdots \tau_t^{m_t},
\end{aligned}$$

where the exponents $a, b, \cdots, m$ are constant rational integers $\geqq 0$, determined by the particular forms of the power products in (3.3), and $\theta^0$ denotes $u$ for all $\theta$ in $AVR$. Since the variables $\xi, \eta, \cdots, \zeta$ are independent in $AVR$, and (say) $\xi = (\xi_1, \cdots, \xi_n)$, $\eta = (\eta_1, \cdots, \eta_n)$, $\cdots$, $\zeta = (\zeta_1, \cdots, \zeta_n)$, the variables $\xi_j, \eta_j, \cdots, \zeta_j (j = 1, \cdots, n)$ are independent in $R$. But these are precisely the independent variables in (3.4). Since each of (3.3), (3.4) implies the other, the complete solution of (3.3) yields all sets of integers (elements of $R$) satisfying (3.4) when $\xi_j, \eta_j, \cdots, \zeta_j$ are equated respectively to the $j$th coordinates in the above power products giving the general solution $\xi, \eta, \cdots, \zeta$ of (3.3). The $j$th coordinates in question are written down as explained in §2, and are polynomials, with rational integer coefficients, in the coordinates of the $\rho, \sigma, \cdots, \tau$. But these coordinates are parameters in $R$.

---

* In this simple example, all solutions $(\alpha, \beta, \gamma, \delta) = (\alpha_1\sigma, \gamma_1\tau, \gamma_1\sigma, \alpha_1\tau)$ are run through once only as coprime $\alpha_1, \gamma_1$ and arbitrary $\sigma, \tau$ run through the elements of $AVR$. But in more complicated equations, the same solution may be given more than once. This however does not affect the statement that *all* solutions are given.

6. It remains to be shown that the theory is not vacuously true. For this it is sufficient to produce instances of $AVR$.

Let $R(\omega) \equiv R(\omega_1, \cdots, \omega_n)$ be an algebraic extension of $R$, and let $\omega_1, \cdots, \omega_n$ be a basis of $R(\omega)$ with the multiplication table

$$\omega_r\omega_s = \sum_{j=1}^{n} \phi(r, s, j)\omega_j.$$

If now $\omega_1 = u$, we may write

$$x(i) = \sum_{j=1}^{n} x(i, j)\omega_j.$$

If in particular $R(\omega)$ is the ring of all algebraic integers in an algebraic number field (relative to the rational field), $\omega_1 = 1$, and the $x(i)$ run through all integers of the field. Hence, if the field is such that unique factorization (without the introduction of ideals) holds, it is an instance of $AVR$. It can be shown conversely that any $AVR$ is isomorphic with an algebraic integer ring.

If in the algebraic integer ring $R(\omega)$ there is not unique factorization, we replace the integers by the principal ideals which they generate; §4 is then applicable. But the application to (3.3) as in §5 does not then yield the solution of (3.4) *practically*, although it does *theoretically*, on account of the following elementary difficulty in the theory of ideals: Given the bases of two *general* ideals $A, B$ to *exhibit* the basis of their product in terms of the $2n$ integers defining the bases of $A, B$. The use of canonical two-term bases does not remove the difficulty. If *general* in the preceding be replaced by *specific*, so that the bases of $A, B$ are expressed in terms of *given* integers, the problem, so far as it concerns algebraic numbers, is solvable in a finite number of steps. But in that case, there is no diophantine problem (3.3) or (3.4). The general existence proof concerning a basis of $R(\omega)$ seems to lead to nothing usable for diophantine analysis.

7. The system (3.3) and its equivalent (3.4) are more restricted than is necessary. Each power product in (3.3) may be replaced by an arbitrary constant integer multiple of itself. For the discussion of (3.3) in this more general case we refer to an article in the Bulletin of the American Mathematical Society for 1933. By referring to §3 it is easily seen what the corresponding (3.4) has become: arbitrary integer coefficients are introduced.

In the papers cited, several illustrative examples of (3.3) have been given, and any desired number can be written out. In conjunction with any algebraic number field in which there is unique factorization, any such example

gives a polynomial diophantine system and its complete solution. An example is given presently.

In the second paper cited, systems not in the form (3.3) but reducible to that form by linear homogeneous substitutions on the variables, with integer coefficients, were discussed. For example, $x^2+y^2=w^2$, $x^2+y^2=w^2+t^2$, and

$$(x+y+w)^3+t^3+v^3+r^3=(t+v+r)^3+x^3+y^3+z^3.$$

Such transformed (3.3) are completely solvable, and hence also the corresponding transformed (3.4).

The notation developed in §3 for the $j$th coordinate in any power product in $VR$ enables us to state in concise form the system (3.4) equivalent to a given (3.3) and to write down the complete solution of a specific system (3.4) from the complete solution of the equivalent (3.3). The last is obtained directly by the algorithm of reciprocal arrays. If the explicit polynomial expressions of the coordinates are required, they are given (for a fixed base $\phi$) by the first formula in §3. A simple example, where (3.3) consists of only one equation, will suffice.

The complete solution in $A\,\Omega$ of the equation

$$x^3 = ytw \tag{7.1}$$

is found by the method of arrays to be

$$\begin{aligned} x &= mabcfghpqr,\\ y &= mgh(af)^2p^3,\\ t &= mca(bg)^2q^3,\\ w &= mbf(ch)^2r^3, \end{aligned} \tag{7.2}$$

where $m, a, b, c, f, g, h, p, q, r$ are parameters ranging independently over all elements of $A\,\Omega$. We shall omit the G.C.D. conditions which may be imposed if desired, as they do not affect the generality of the solution.

By a mere change of notation (7.1) becomes (7.3) in $AVR$,

$$v^3(x) = v(y)v(t)v(w), \tag{7.3}$$

which is equivalent in $R$ to the simultaneous system (corresponding to (3.4)),

$$v(x^3; j) = v(y, t, w; j) \qquad (j = 1, \cdots, n). \tag{7.4}$$

The $j$th coordinates written in (7.4) are homogeneous polynomials in $R$ of degree 3, whose explicit forms can be written down by the first formula in §3. The complete solution of (7.4) is written down similarly from (7.2):

$$v(x;j) = v(m, a, b, c, f, g, h, p, q, r; j),$$
$$v(y;j) = v(m, g, h, a^{(2)}, f^{(2)}, p^{(3)}),$$
$$v(t;j) = v(m, c, a, b^{(2)}, g^{(2)}, q^{(3)}),$$
$$v(w;j) = v(m, b, f, c^{(2)}, h^{(2)}, r^{(3)}) \qquad (j = 1, \cdots, n).$$

Thus the $4n$ independent variables in (7.4) are given parametrically in the complete solution in terms of $10n$ integer parameters.

For the complete solution of a given system (3.4) equivalent to (3.3) in an $AVR$ which is algebraic of degree $n$ it is necessary to select algebraic number fields of degree $n$ in which there is unique factorization, and to construct the multiplication table $\omega_r\omega_s(r, s=1, \cdots, n)$ for the basis, in order to get the $\phi(r, s, j)(j=1, \cdots, n)$. For $n=2$, 3, 4 only is there sufficient knowledge extant to enable us to obtain the general $\phi$. For no $n$ is it known in all of what fields of that degree there is unique factorization; if $n=2$ any field with class number 1 may be used, but not all such fields are known; if $n=3$ there are numerous special fields known. For $n \geqq 4$, the $\phi$ can also be obtained for some special fields. Although there is nothing approaching generality in the available data concerning algebraic fields which is necessary for the application to diophantine analysis, nevertheless an infinity of completely solvable polynomial diophantine systems exist, and any number can be constructed from a single algebraic $AVR$ alone.

As the entire subject originated in the Pythagorean equation $x^2+y^2=t^2$, we shall state the most general system equivalent to this and solvable completely in rational integers by the methods of this paper. Let $d$ denote a non-zero rational integer, and for simplicity restrict $d$ to have no square factor $>1$ (a restriction easily removed). Write $D=4d$ if $d\equiv 2$ or 3 mod 4, $D=d$ if $d\equiv 1$ mod 4; $B=-\frac{1}{4}D(D-1)$. Then $B$ is a rational integer. Let the field generated by $d^{1/2}$ have class number 1. Then the system in question is

$$x_1^2 + y_1^2 - z_1^2 - w_1^2 + B(x_2^2 + y_2^2 - z_2^2 - w_2^2) = 0,$$
$$2(x_1x_2 + y_1y_2 - z_1z_2 - w_1w_2) + D(x_2^2 + y_2^2 - z_2^2 - w_2^2) = 0.$$

As the complete solution of this in rational integers $x_j, y_j, z_j, w_j$ $(j=1, 2)$ is somewhat more detailed than that of the next, which is equivalent to it, we shall conclude with the complete solution in rational integers $\xi_i, \eta_i, \lambda_i, \mu_i$ $(i=1, 2)$ of the system

$$\xi_1\xi_2 + B\eta_1\eta_2 = \lambda_1\lambda_2 + B\mu_1\mu_2,$$
$$\xi_1\eta_2 + \xi_2\eta_1 + D\eta_1\eta_2 = \lambda_1\mu_2 + \lambda_2\mu_1 + D\mu_1\mu_2.$$

Let the $\alpha_j, \beta_j(j=1, \cdots, 4)$ be parameters ranging over all rational integers independently. Then the complete solution is

$$\xi_1 = \alpha_1\alpha_3 + B\beta_1\beta_3, \quad \eta_1 = \alpha_1\beta_3 + \alpha_3\beta_1 + D\beta_1\beta_3,$$
$$\xi_2 = \alpha_2\alpha_4 + B\beta_2\beta_4, \quad \eta_2 = \alpha_2\beta_4 + \alpha_4\beta_2 + D\beta_2\beta_4,$$
$$\lambda_1 = \alpha_1\alpha_4 + B\beta_1\beta_4, \quad \mu_1 = \alpha_1\beta_4 + \alpha_4\beta_1 + D\beta_1\beta_4,$$
$$\lambda_2 = \alpha_2\alpha_3 + B\beta_2\beta_3, \quad \mu_2 = \alpha_2\beta_3 + \alpha_3\beta_2 + D\beta_2\beta_3.$$

This follows at once, by the algorithm described, from the solution of $\alpha\beta=\gamma\delta$ in §5. Note that nothing has been proved if the class number exceeds unity.

Finally it may be stated that the number of parameters appearing in any solution obtained by the algorithm is both necessary and sufficient for the complete solution. This is a consequence of the like for any application of reciprocal arrays.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.