REDUCIBLE DIOPHANTINE EQUATIONS AND THEIR PARAMETRIC REPRESENTATIONS

E. ROSENTHALL

1. Reducible diophantine equations. The present paper will provide a general method for obtaining the complete parametric representation for the rational integer solutions of the multiplicative diophantine equation

$$1.1 \qquad \prod_{(k)} \prod_{i=1}^{q} \prod_{j=1}^{p} [f_{ki}(x_{1ji}, \ldots, x_{kji})]^{a_{ijk}} = \prod_{(k)} \prod_{i=1}^{q} \prod_{j=1}^{p} [h_{ki}(y_{1ji}, \ldots, y_{kji})]^{b_{ijk}}$$

for some specified range of k, where the a_{ijk}, b_{ijk} are non-negative integers and the f_{ki}, h_{ki} are decomposable forms, that is to say they are integral irreducible homogeneous polynomials over the rational field R of degree k in k variables which can be written as the product of k linear forms.

Equations of the form 1.1 appear often in diophantine problems and many results concerning their parametric solutions are known. An account of some of these has been given by Skolem **(6**, pp. 64–69**)** where the most general equation of type 1.1 considered is

$$1.2 \qquad f(x_1, x_2, \ldots, x_n) = hy_1^{e_1} y_2^{e_2} \ldots y_p^{e_p},$$

f being a decomposable form of degree n, and we note that 1.1 becomes 1.2 when we restrict the a_{ijk}, b_{ijk} so that $a_{11n} = 1$; $a_{ijk} = 0$ when $i \neq 1$, $j \neq 1$, $k \neq n$; $b_{1j1} = e_j$; $b_{ijk} = 0$ when $i \neq 1$, $k \neq 1$.

The method illustrated there for the complete resolution of 1.2 uses ideal theory in the ring of integers of the algebraic number field K in which f splits, i.e. the field in which f can be written as the product of linear factors. In this process, by solving a simple multiplicative equation **(3**, p. 87**)** in the rational domain, the resolution of 1.2 is reduced to finding all $x_1, x_2, \ldots, x_n$ and $u_1, u_2, \ldots, u_m$ satisfying an equation of the form

$$1.3 \qquad N(\omega_1 x_1 + \omega_2 x_2 + \ldots + \omega_n x_n) = bu_1^{b_1} u_2^{b_2} \ldots u_m^{b_m}$$

with the g.c.d. condition $(x_1, x_2, \ldots, x_n) = 1$ where $\omega_1, \omega_2, \ldots, \omega_n$ is a minimal basis of K and $N(T)$ denotes the norm of the algebraic number T. The resolution of 1.3 is then obtained by factoring each u_i into prime ideals of all permissible degrees and then these prime ideals must be distributed among the linear factors of the left hand member in all possible ways so that these factors are conjugates and the equation is satisfied. No systematic method is provided for making this distribution and although the complete resolution of 1.2 is thus not too difficult in principle the above procedure when applied to 1.2 itself is unwieldy and is certainly unserviceable for the complete resolution of

Received June 14, 1954.

1.1. In view of these circumstances there appears a need for a straightforward method to handle with more facility the general completely reducible equation 1.1.

In this paper we shall consider 1.1 from a different point of view. If f is a decomposable form of degree n then it is well known **(1**, pp. 378–383**)** that a certain integral multiple of f or a form equivalent to f can be expressed as $N(\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n)$ where $\alpha_1, \alpha_2, \ldots \alpha_n$ are integers of an algebraic number field of degree n. It follows that equation 1.1 can be replaced by an equation of the form

$$1.4 \qquad a\prod_{(k)}\prod_{i=1}^{q}\prod_{j=1}^{p}[N(\alpha_{1ki}x_{1ji}+\ldots+\alpha_{kki}x_{kji})]^{a_{ijk}} = b\prod_{(k)}\prod_{i=1}^{q}\prod_{j=1}^{p}[N(\beta_{1ki}y_{1ji}+\ldots+\beta_{kki}y_{kji})]^{b_{ijk}}$$

where α_{rki}, β_{rki} are algebraic integers of degree k and a, b are rational integers. The resolution of 1.1 thus reduces to solving a multiplicative equation in which each member is a product of linear forms in the normal algebraic extension E/R where E is generated by adjoining to R all the α_{rki}, β_{rki} and their conjugates.

The general equation of type 1.4 associated in this form with a given normal extension is formulated below in 2.1 and in the development of our method for the complete resolution of 2.1 it is the Galois group G of the normal extension E which plays a dominant role, and the method permits the equations to be classified according to their group G. We shall show that there is a correspondence between the solutions of 2.1 and the complete parametric representations in multiplicative form of a multiplicative system of independent equations in the rational domain. From a knowledge of these parametric representations, which can be obtained by the method of Bell **(2)** or Ward **(6)**, the complete solution of 2.1 can be written down. The passage from 2.1 to the corresponding multiplicative system in the rational domain and the return from the solutions of this system to the solutions of 2.1 only require the simple and straightforward computation in G as prescribed in Lemma 1. This is established by Theorem 2 and the algorithm in §5.

In an earlier paper the author established Theorem 2 for the case where E is the cyclotomic number field **(4**, p. 219**)**. Although not mentioned in that paper it is readily seen that the same proof shows that this theorem, as stated there, holds for any cyclic field. It was then natural to inquire whether or not a theorem of the same type could be obtained when the Galois group of E is not necessarily cyclic, and to answer this question has led to the present investigation.

2. Notations and conjugate elements. We now introduce some notations and definitions and state a few well-known properties of conjugate elements which are needed in this paper. Let E be a normal algebraic extension of degree n over R and let G be its Galois group; the subgroups of G will be

represented by g, and $o(g)$ stands for the order of g. G can be partitioned into complete conjugate classes $S_1, S_2, \ldots, S_t$ and g_i will denote a representative group from the class S_i. All the small Latin letters will represent rational integers and large Latin letters, unless specified otherwise, will denote ideals in the ring of integers of E. The Greek letters σ, τ, ν are reserved for the substitutions of G. If α is an element of E then $\sigma(\alpha)$, called a conjugate of α, is the image of α under the substitution σ. By σT we mean the ideal obtained from T when we replace each integer α in T by $\sigma(\alpha)$; the ideals σT are called the conjugates of T. All the substitutions of G which leave T unaltered form a group g; we then say that T belongs to g. All the substitutions of G which transform T into a given conjugate element τT form a left coset τg of g. It then follows that all the distinct conjugates of T are given without repetition by $\tau_1 T, \tau_2 T, \ldots, \tau_r T$ where $\tau_1, \tau_2, \ldots, \tau_r$ form a complete set of left residues of G modulo g. Also if T belongs to g then the conjugate ideal σT belongs to $\sigma g \sigma^{-1}$; thus conjugate ideals belong to conjugate subgroups and therefore the only ideals belonging to the set S_j, i.e. to any group of S_j, are the conjugates of ideals belonging to g_j. The letter P will be reserved for prime ideals. $T_{i,k}$ will signify that the ideal T_k belongs to the group g_i.

If $\tau_{i1}, \tau_{i2}, \ldots \tau_{ig(i)}$ be a complete set of left residues of G modulo g_i then with each permissible Galois group G we can associate the multiplicative equation

$$2.1 \qquad \prod_{k=1}^{h} \prod_{i=1}^{t} [\tau_{i1} X_{i,k} \tau_{i2} X_{i,k} \ldots \tau_{ig(i)} X_{i,k}]^{a_{ik}} = \prod_{k=1}^{h} \prod_{i=1}^{t} [\tau_{i1} Y_{i,k} \ldots \tau_{ig(i)} Y_{i,k}]^{b_{ik}}$$

where a_{ik}, b_{ik} are non-negative integers.

Theorem 2 provides a method for the resolution of 2.1 yielding the solution in multiplicative form. If further we select the ideal parameters in this solution of 2.1 so that the ideals X_k and Y_k are principal we obtain the complete solution of 1.4 in rational integers.

3. Lemmas. The following lemmas are required.

LEMMA 1. *Form the following array containing all the left residues of G modulo g_j:*

$$\begin{array}{l} \nu_{11,ij}\, \nu_{12,ij} \ldots \nu_{1\,a(1),ij} \\ \nu_{21,ij}\, \nu_{22,ij} \ldots \nu_{1\,a(2),ij} \\ \nu_{s(i,j)1,ij} \ldots \nu_{s(i,j)a(s),ij} \end{array}$$

where $\nu_{e1;ij}$ is a left residue modulo g_j not in the first $e-1$ rows and the elements of the eth row are all the distinct left residues modulo g_j of the elements of the right coset $g_i \nu_{e1;ij}$.

Then if A is an ideal belonging to g_j all the distinct conjugates of A are given without repetition by

$$\nu_{ef;ij} A$$

for $e = 1, 2, \ldots, s(i,j); f = 1, 2, \ldots, a(e)$.

This follows since the array contains all the left residues of G modulo g_j and no residue appears twice.

In §6 we shall refer to the above array as the $\nu(i, j)$ array for G.

LEMMA 2. *Let A be unaltered by g_i and let B be the product of all prime ideals belonging to the conjugate set S_j which divide A. Then B can be expressed in the form*

$$\prod_{r=1}^{v} \prod_{e=1}^{s(i,j)} \left(\prod_{f=1}^{a(e)} \nu_{ef,ij} P_{j,r} \right)^{c_{re}},$$

where the ν are as described in Lemma 1 and the c_{re} are non-negative integers.

Proof. Since the only primes belonging to the conjugate set S_j are the conjugates of ideals belonging to g_j then by Lemma 1, B must be of the form

$$B = \prod_{r=1}^{v} \left(\prod_{e=1}^{s(i,j)} \prod_{f=1}^{a(e)} \nu_{ef,ij} P_{j,r} \right)^{d_{ref}}.$$

But B is the product of all primes belonging to the same conjugate set which divide an ideal which is unaltered by g_i and so B is also unaltered by g_i. It follows then that if $\nu_{e1;ij} P_{j,r}$ divides B so does $\sigma\nu_{e1,ij} P_{j,r}$ for each $\sigma \in g_i$. However not all these divisors are distinct. The distinct images of $P_{j,r}$ by the substitutions of the coset $g_i \nu_{e1,ij}$ are those obtained by the distinct left residues of $g_i \nu_{ei,ij}$ modulo g_j, i.e. by the substitutions $\nu_{e1,ij}, \nu_{e2,ij}, \ldots, \nu_{ea(a),ij}$. Hence $d_{re1} = d_{re2} = \ldots = d_{rea(e)} = c_{re}$, say since by Lemma 1 the conjugates $\nu_{ef,ij} P_{j,r}$ are all distinct.

LEMMA 3. *Any left residue of G modulo g_j which appears in the coset τg_i occurs there with multiplicity equal to $o(g_i \cap g_j)$.*

Proof. If σ is in the intersection of the cosets τg_i and σg_j then these cosets both contain $\sigma\nu$ for all $\nu \in g_i \cap g_j$, and these are the only elements in their intersection.

LEMMA 4. *Let $\tau_1, \tau_2, \ldots, \tau_a$ be a complete set of left residues of G modulo g_i and let $\sigma_1, \sigma_2, \ldots, \sigma_b$ be a complete set of left residues of g_i modulo g_j. Then among the products $\tau_r \sigma_s$ $(r = 1, \ldots, a;\ s = 1, \ldots, b)$ appear all the left residues of G modulo g_j and each residue occurs with multiplicity $o(g_j)/o(g_i \cap g_j)$.*

Proof. The cosets $\tau_r g_i$ $(r = 1, 2, \ldots, a)$ contain all the left residues of G modulo g_j each with multiplicity $o(g_j)$. In each coset $\tau_r g_i$ a given left residue modulo g_j which appears there occurs, by Lemma 3, with multiplicity $o(g_i \cap g_j)$. Hence a given left residue of G modulo g_j must appear in $o(g_j)/o(g_i \cap g_j)$ of the cosets $\tau_r g_i$. Since all the residues $\tau\sigma_1, \ldots, \tau\sigma_b$ for given τ are distinct modulo g_j and they are all the distinct left residues of τg_i, the theorem follows.

LEMMA 5. *Let $\tau_1, \ldots, \tau_a$ be a complete set of left residues of G modulo g_i and let $\sigma_1\nu, \ldots, \sigma_b\nu$ for $\sigma \in g_i$ be a complete set of left residues of $g_i\nu$ modulo g_j.*

https://doi.org/10.4153/CJM-1955-036-0 Published online by Cambridge University Press

Then among the products $\tau_r \sigma_s$ $(r = 1, \ldots, a;\ s = 1, \ldots, b)$ *appear all the left residues of* G *modulo* $\nu g_j \nu^{-1}$ *each appearing with multiplicity*

$$o(g_j)/o(g_i \cap \nu g_j \nu^{-1}).$$

This follows from Lemma 4, since $\sigma_1, \sigma_2, \ldots, \sigma_b$ is a complete set of left residues of g_i modulo $\nu g_j \nu^{-1}$.

4. Fundamental theorem. We introduce some additional notation. The notation $A_{j;ik}$ denotes that ideal A_k is the product of all ideals belonging to the conjugate set S_j which divide an ideal unaltered by g_i, and $\tau_{i1}, \ldots, \tau_{ig(i)}$ denotes a complete set of left residues of G modulo g_i; $\gamma(m, ij)$ will denote the quotient

$$o(g_j)/o(g_i \cap \nu_{m1,ij}\, g_j\, \nu^{-1}{}_{m1,ij}),$$

where the ν are as prescribed in Lemma 1; also $s(i, j)$, which we shall denote by s in this section, is as defined in Lemma 1.

THEOREM 1. *All solutions of*

$$4.1 \qquad \prod_{k=1}^{h} \prod_{i=1}^{t} (\tau_{i1} A_{j;ik} \ldots \tau_{ig(i)} A_{j;ik})^{a_{ik}} = \prod_{k=1}^{h} \prod_{i=1}^{t} (\tau_{i1} B_{j;ik} \ldots \tau_{ig(i)} B_{j;ik})^{b_{ik}}$$

are given by

$$4.2 \qquad A_{j;ik} = \prod_{q=1}^{w} \prod_{e=1}^{s} (Y_{j,q}^{(e)})^{m_{qe,ik}}, \quad B_{j;ik} = \prod_{q=1}^{w} \prod_{e=1}^{s} (Y_{j,q}^{(e)})^{n_{qe,ik}}$$

where

$$Y_{j,q}^{(e)} = \nu_{e1,ij} T_{j,q} \ldots \nu_{ea(e)} T_{j,q}$$

and

$$m_{q1,ik}, \ldots, m_{qs,ik};\ n_{q1,ik}, \ldots, n_{qs,ik} \qquad (q = 1, 2, \ldots, w)$$

are all the distinct primitive solutions x, y *of the linear system*

$$4.3 \qquad \sum_{k=1}^{h} \sum_{i=1}^{t} \sum_{e=1}^{s} a_{ik} \gamma(e, ij)\, x_{e,ik} = \sum_{k=1}^{h} \sum_{i=1}^{t} \sum_{e=1}^{s} b_{ik} \gamma(e, ij)\, y_{e,ik}.$$

Proof. From Lemma 2 it is seen that $A_{j;ik}$ is of the form

$$4.4 \qquad A_{j;ik} = \prod_{r=1}^{v} \prod_{e=1}^{s} \left(\prod_{f=1}^{a(e)} \nu_{ef,ij} P_{j,r} \right)^{c_{re,ik}}$$

and there is a similar expression for $B_{j;ik}$ with $c_{re,ik}$ replaced by $d_{re,ik}$. Substituting 4.4 in 4.1 gives

$$\prod_{k=1}^{h} \prod_{i=1}^{t} \prod_{r=1}^{v} \prod_{e=1}^{s} \prod_{f=1}^{a(e)} \prod_{b=1}^{g(i)} (\tau_{ib} \nu_{ef,ij} P_{j,r})^{a_{ik} c_{re,ik}} = \prod_{k=1}^{h} \prod_{i=1}^{t} \prod_{r=1}^{v} \prod_{e=1}^{s} \prod_{f=1}^{a(e)} \prod_{b=1}^{g(i)} (\tau_{ib} \nu_{ef,ij} P_{j,r})^{b_{ik} d_{re,ik}}$$

which by Lemma 5 becomes

https://doi.org/10.4153/CJM-1955-036-0 Published online by Cambridge University Press

$$4.5 \qquad \prod_{k=1}^{h}\prod_{i=1}^{t}\prod_{r=1}^{v}\prod_{e=1}^{s}[\tau_{j1}P_{j,r}\ldots\tau_{jg(j)}P_{j,r}]^{a_{ik}\gamma(e,ij)c_{re,ik}} = \prod_{k=1}^{h}\prod_{i=1}^{t}\prod_{r=1}^{v}\prod_{e=1}^{f}[\tau_{j1}P_{j,r}\ldots\tau_{jg(j)}P_{j,r}]^{b_{ik}\gamma(e,ij)d_{re,ik}},$$

and this is equivalent to

$$\prod_{k=1}^{h}\prod_{i=1}^{t}\prod_{r=1}^{v}[\tau_{j1}P_{j,r}\ldots\tau_{jg(j)}P_{j,r}]^{a_{ik}c_{r,ik}} = \prod_{k=1}^{h}\prod_{i=1}^{t}\prod_{r=1}^{v}[\tau_{j1}P_{j,r}\ldots\tau_{jg(j)}P_{j,r}]^{b_{ik}d_{r,ik}},$$

where

$$c_{r,ik} = \sum_{e=1}^{s} c_{re,ik}\gamma(e,ij), \quad d_{r,ik} = \sum_{e=1}^{s} d_{re,ik}\gamma(e,ij).$$

This relationship is satisfied if and only if

$$4.6 \qquad \sum_{k=1}^{h}\sum_{i=1}^{t} a_{ik}c_{r,ik} = \sum_{k=1}^{h}\sum_{i=1}^{t} b_{ik}d_{r,ik} \qquad (r = 1, 2, \ldots, v).$$

This is a linear system of equations to be solved for the non-negative integers $c_{re,ik}$, $d_{re,ik}$. For fixed r let the w primitive solutions **(5**; p. 9**)** be

$$m_{q1,ik}, \ldots, m_{qs,ik}; \; n_{q1,ik}, \ldots, n_{qs,ik}$$

for $i = 1, 2, \ldots, t$; $k = 1, 2, \ldots, h$ and $q = 1, 2, \ldots, w$. Then all non-negative solutions of 4.6 are given by

$$4.7 \qquad c_{re,ik} = \sum_{q=1}^{w} u_{qr}m_{qe,ik}, \quad d_{re,ik} = \sum_{q=1}^{w} u_{qr}n_{qe,ik}$$

for integer parameters u_{qr}. Substituting 4.7 in 4.4 and putting

$$\prod_{r=1}^{v}(P_{j,r})^{u_{qr}} = T_{j,q}$$

we get

$$A_{j;ik} = \prod_{q=1}^{w}\prod_{e=1}^{s}\prod_{f=1}^{a(e)}(\nu_{ef,ij}T_{j,r})^{m_{qe,ik}}, \quad B_{j;ik} = \prod_{q=1}^{w}\prod_{e=1}^{s}\prod_{f=1}^{a(e)}(\nu_{ef,ij}T_{j,r})^{n_{qe,ik}},$$

which we can write as

$$A_{j;ik} = \prod_{q=1}^{w}(Y_{j,q}^{(1)})^{m_{q1,ik}}(Y_{j,q}^{(2)})^{m_{q2,ik}}\ldots(Y_{j,q}^{(s)})^{m_{qs,ik}}$$

and similar expression for $B_{j;ik}$ with $m_{ql,ik}$ replaced by $n_{ql,ik}$.

THEOREM 2. *Let the complete solution in multiplicative form of the equation*

$$4.8 \qquad \prod_{k=1}^{h}\prod_{i=1}^{t}\prod_{e=1}^{s} x_{e,ik}^{\gamma(e,ij)a_{ik}} = \prod_{k=1}^{h}\prod_{i=1}^{t}\prod_{e=1}^{s} y_{e,ik}^{\gamma(e,ij)b_{ik}}$$

in the rational domain be

$$4.9 \qquad x_{e,ik} = \prod_{q=1}^{w} t_q^{m_{qe,ik}}, \quad y_{e,ik} = \prod_{q=1}^{w} t_q^{n_{qe,ik}} \qquad (e = 1, 2, \ldots, s).$$

https://doi.org/10.4153/CJM-1955-036-0 Published online by Cambridge University Press

Then the complete solution of (4.1) *is given by*

$$A_{j;ik} = \prod_{e=1}^{s} x_{e,ik}, \quad B_{j;ik} = \prod_{e=1}^{s} y_{e,ik},$$

where $x_{e,ik}$, $y_{e,ik}$ *are as stated in* 4.9 *but with* t_q *replaced by*

$$Y_{j,q}^{(e)} = \nu_{e1,ij} T_{j,q} \ldots \nu_{ea(e),ij} T_{j,q}.$$

Proof. If 4.9 is the complete solution in multiplicative form of 4.8 then $m_{qe,ik}$ and $n_{qe,ik}$ are the primitive solutions of equation 4.3 **(6**, p. 70**)**. Thus the values of $A_{j;ik}$ and $B_{j;ik}$ in 4.1 are precisely the relations 4.2.

5. The algorithm. We can now furnish a procedure for the resolution of the ideal equation

$$5.1 \qquad \prod_{k=1}^{h} \prod_{i=1}^{t} (\tau_{i1} X_{i,k} \tau_{i2} X_{i,k} \ldots \tau_{ig(i)} X_{i,k})^{a_{ik}} = \prod_{k=1}^{h} \prod_{i=1}^{t} (\tau_{i1} Y_{i,k} \tau_{i2} Y_{i,k} \ldots \tau_{ig(i)} Y_{i,k})^{b_{ik}}$$

With $A_{j;ik}$ as defined in §4 we can write

$$5.2 \qquad X_{i,k} = \prod_{j=1}^{t} A_{j;ik}, \quad Y_{i,k} = \prod_{j=1}^{t} B_{j;ik}.$$

Substituting 5.2 into 5.1, and since a given prime ideal belongs to only one conjugate set, we can equate the product of primes belonging to the same conjugate set and we get the system

$$5.3 \qquad \prod_{k=1}^{h} \prod_{i=1}^{t} (\tau_{i1} A_{j;ik} \tau_{i2} A_{j;ik} \ldots \tau_{ig(i)} A_{j;ik})^{a_{ik}} = \prod_{k=1}^{h} \prod_{i=1}^{t} (\tau_{i1} B_{j;ik} \tau_{i2} B_{j;ik} \ldots \tau_{ig(i)} B_{j;ik})^{b_{ik}} \qquad (j = 1, 2, \ldots, t).$$

Each equation of this system is of the type 4.1 and can be solved by the method given there. Substituting the expressions found in this way for $A_{j;ik}$, $B_{j;ik}$ into 5.2 gives the complete solution in multiplicative form of the ideal equation 5.1.

Remark. Theorem 2 was stated and proved only for the case when 4.1 and hence the associated system 4.8 consists of two equal products. However the theorem also holds when 4.1 consists of a finite number of equal products. This follows since Ward's result on the correspondence of the solutions of additive and multiplicative equations holds for multiplicative systems with a finite number of equal products.

It will also be seen from the example considered in §6 that the number of parameters in the complete solution of 5.1 obtained here can be reduced. No general results are given here which will yield the solution in terms of a minimum number of parameters.

6. Example. For purposes of illustrating the algorithm we shall consider a very simple equation, one which splits in a field with group $G\ (1, \sigma)$ where $\sigma^2 = 1$. Representatives from each of the complete conjugate sets are $g_1 = G$, $g_2 = 1$.

Let us consider the problem of solving completely the ideal equation which arises in the complete resolution in rational integers of the equation $x^2+ay^2=z^n$, namely,

$$X_{2,1}.\sigma X_{2,1} = Y_{1,1}^n. \tag{6.1}$$

Putting

$$X_{2,1} = A_{1;21}\,A_{2;21} \text{ and } Y_{1,1} = B_{1;11}\,B_{2;11}, \tag{6.2}$$

then for equation (6.1) the relations (5.3) become

$$A_{j;21}.\sigma A_{j;21} = B_{j;11}^n \qquad (j = 1, 2),$$

and these equations must be solved for each j. For this purpose we require the $\nu(1, j)$ and $\nu(2, j)$ sets as defined in Lemma 1 and the corresponding multiplicative equation in the rational domain with its parametric solution. This data is listed below for $j = 1, 2$ and the corresponding values of $A_{j;21}$, $B_{j;11}$ are at once written down.

$$\begin{aligned}
j = 1.\quad & \nu_{11,11} = 1; \quad s(1, 1) = 1, \gamma(1, 11) = 1.\\
& \nu_{11,21} = 1; \quad s(2, 1) = 1, \gamma(1, 21) = 2.\\
& x_{1,21}^2 = y_{1,11}^n \rightarrow x_{1,21} = t_1^n, \qquad y_{1,21} = t_1^2.\\
& A_{1;21} = T_{1,1}^n \qquad B_{1;11} = T_{1,1}^2.\\
j = 2.\quad & \nu_{11,12} = 1, \qquad \nu_{12,12} = \sigma; \ s(1, 2) = 1, \gamma(1, 12) = 1.\\
& \nu_{11,22} = 1\\
& \nu_{21,22} = \sigma; \qquad s(2, 2) = 2, \gamma(1, 22) = 1, \gamma(2, 22) = 1.\\
& x_{1,21}x_{2,21} = y_{1,11}^n \rightarrow x_{1,21} = t_1^n t_2^{n-1} \ldots t_n,\\
& \qquad\qquad x_{2,21} = t_2 t_3^2 \ldots t_{n+1}^n,\\
& \qquad\qquad y_{1;11} = t_1 t_2 \ldots t_{n+1}.\\
& A_{2;21} = T_{2,1}^n T_{2,2}^{n-1} \ldots T_{2,n}.\sigma(T_{2,2}T_{2,3}^2 \ldots T_{2,n+1}^n),\\
& B_{2;11} = T_{2,1}T_{2,2} \ldots T_{2,n+1}.\sigma(T_{2,1}T_{2,2} \ldots T_{2,n+1}).
\end{aligned}$$

Substituting these expression for $A_{j;21}$, $B_{j;11}$ into (6.2) yields the following for the complete solution of (6.1),

$$\begin{aligned}
X_{2,1} &= T_{1,1}^n(T_{2,1}^n T_{2,2}^{n-1} \ldots T_{2,n}).\sigma(T_{2,2}T_{2,3}^2 \ldots T_{2,n+1}^n),\\
Y_{1,1} &= T_{1,1}^2(T_{2,1}T_{2,2} \ldots T_{2,n+1}).\sigma(T_{2,1}T_{2,2} \ldots T_{2,n+1}).
\end{aligned}$$

In conclusion we list the result obtained when the method of this paper is applied to an equation which splits in a field whose group G is the group of

https://doi.org/10.4153/CJM-1955-036-0 Published online by Cambridge University Press

symmetries of the square. G is then a group of order eight generated by σ, τ where $\tau^2 = \sigma^4 = 1$, $\tau\sigma = \sigma^3\tau$, $\tau\sigma^2 = \sigma^2\tau$, $\tau\sigma^3 = \sigma\tau$. Representatives from each of the complete conjugate sets can be taken to be $g_1 = G, g_2 = (1, \sigma, \sigma^2, \sigma^3)$, $g_3 = (1, \sigma^2, \tau, \sigma^2\tau)$, $g_4 = (1, \sigma^2, \sigma\tau, \sigma^3\tau)$, $g_5 = (1, \sigma^2)$, $g_6 = (1, \tau)$, $g_7 = (1, \sigma\tau)$, $g_8 = \tau$.

Then by the method of this paper the complete solution of the ideal equation

$$X_{6,1} \cdot \sigma X_{6,1} \cdot \sigma^2 X_{6,1} \cdot \sigma^3 X_{6,1} = U_{2,1} \cdot \tau U_{2,1} \tag{6.3}$$

is found to be

$$X_{6,1} = N_{2,3}^{1+\tau} N_{3,2} N_{8,1}^{1+\tau}$$

$$U_{2,1} = N_{2,3}^{3+\tau} N_{3,2}^{1+\sigma} N_{8,1}^{1+\sigma+\sigma^2+\sigma^3},$$

where the notation $T^{a\sigma+b\tau}$ is used for $\sigma T^a \cdot \tau T^b$. Equation 6.3 arises, for example, in the complete resolution in rational integers of the equation

$$N(a + b\theta + c\theta^2 + d\theta^3) = u^2 + v^2$$

where $\theta = \sqrt[4]{a}$.

References

1. P. Bachman, *Die Arithmetik der quadratischen Formen* (Berlin, 1923).
2. E. T. Bell, *Reciprocal arrays and diophantine analysis*, Amer. J. Math., *55* (1933), 50–66.
3. ———, *Separable diophantine equations*, Trans. Amer. Math. Soc., *57* (1945), 86–101.
4. E. Rosenthall, *Diophantine equations separable in cyclotomic fields*, Duke Math. J. *20* (1953), 141–338.
5. T. Skolem, *Diophantische Gleichungen*, Ergebnisse der Math. und ihrer Grenzgebiete, *5*, no. 4 (Berlin, 1938).
6. Morgan Ward, *A type of multiplicative diophantine system*, Amer. J. Math., *55* (1933), 67–76.

McGill University