ON THE APPLICATION OF THE THEORY OF IDEALS TO DIOPHANTINE ANALYSIS*

BY G. E. WAHLIN

1. *Introduction.* About three years ago† Professor Dickson stated a certain conjectured theorem, and he has recently published a proof of it.‡

After having examined a proof of the same theorem by the author of this article, Professor Dickson suggested the investigation of a more general equation than the one which he had considered, and the following pages contain the results of this investigation.

2. *Rings.* Let us consider any algebraic number field $k(\theta)$ of degree n. Let $\gamma_1, \gamma_2, \ldots, \gamma_n$ be a fundamental system of integers of $k(\theta)$ so that every integer of the field can be represented by the fundamental form

$$x_1\gamma_1 + x_2\gamma_2 + \cdots + x_n\gamma_n, \tag{1}$$

in which the $x_1, x_2, \ldots, x_n$ are rational integers.

By a *ring* R in $k(\theta)$ we understand a set of integers which is closed with respect to addition, subtraction, and multiplication, and which contains the rational integers. Let $\varrho_1, \varrho_2, \ldots, \varrho_n$ be a fundamental system of R. As above, we shall call

$$x_1\varrho_1 + x_2\varrho_2 + \cdots + x_n\varrho_n \tag{2}$$

the *fundamental form* of R. Every element of R is represented once and only once by (2) when the $x_1, x_2, \cdots, x_n$ are given rational integral values.

Since $\varrho_1, \varrho_2, \ldots, \varrho_n$ are integers in $k(\theta)$, they can be represented by (1), and we shall suppose that

$$\varrho_i = r_{i1}\gamma_1 + r_{i2}\gamma_2 + \cdots + r_{in}\gamma_n, \qquad (i = 1, 2, \ldots, n). \tag{3}$$

* Presented to the Society, December 29, 1923.

† L. E. Dickson, *A new method in Diophantine analysis,* this BULLETIN, vol. 27, No. 8 (May, 1921), p. 353.

‡ L. E. Dickson, *Integral solutions of $x^2 - my^2 = zw$,* this BULLETIN, vol. 29, No. 10 (Dec., 1923), p. 464.

The absolute value of the determinant $|r_{ij}|$ of the system (3) shall be called the *index of the ring,* and shall be denoted by Δ. Since any product of integers of R belongs to R the product

$$\varrho_1^{s_1} \cdot \varrho_2^{s_2} \cdots \varrho_n^{s_n}, \quad s_i \geqq 0, \qquad (i = 1, 2, \ldots, n)$$

can be represented by (2), and we shall write

$$(4) \quad \varrho_1^{s_1} \cdot \varrho_2^{s_2} \cdots \varrho_n^{s_n} = C^{(1)}_{s_1 s_2 \ldots s_n} \varrho_1 + C^{(2)}_{s_1 s_2 \ldots s_n} \varrho_2 + \cdots + C^{(n)}_{s_1 s_2 \ldots s_n} \varrho_n.$$

This equation uniquely defines the rational integers $C^{(i)}_{s_1 s_2 \ldots s_n}$.

Let us next consider any k integers $\alpha', \alpha'', \ldots, \alpha^k$ from R, and let

$$\alpha^{(i)} = a_{1i}\varrho_1 + a_{2i}\varrho_2 + \cdots + a_{ni}\varrho_n, \qquad (i = 1, 2, \ldots, k).$$

We may then write the product

$$(5) \qquad \alpha' \cdot \alpha'' \cdots \alpha^{(k)} = \sum B_{s_1 s_2 \ldots s_n} \varrho_1^{s_1} \cdot \varrho_2^{s_2} \cdots \varrho_n^{s_n},$$

where the summation extends over all terms for which $s_1 + s_2 + \cdots + s_n = k$, and

$$B_{s_1 s_2 \ldots s_n} = \sum a_{1 i_{11}} \cdots a_{1 i_{1 s_1}} \cdot a_{2 i_{21}} \cdots a_{2 i_{2 s_2}} \cdot \cdots \cdot a_{n i_{n s_n}}.$$

That is, $B_{s_1 s_2 \ldots s_n}$ is the sum of all possible products formed by taking s_1 elements from the first column, s_2 from the second, s_3 from the third, etc., and so chosen that no two elements belong to the same row in the matrix

$$m = \left\| \begin{matrix} a_{11}, & a_{21}, & \ldots, & a_{n1} \\ a_{12}, & a_{22}, & \ldots, & a_{n2} \\ \cdot & \cdot & \cdot & \cdot \\ a_{1k}, & a_{2k}, & \ldots, & a_{nk} \end{matrix} \right\|.$$

If in (5) we now replace the power-products $\varrho_1^{s_1} \cdot \varrho_2^{s_2} \cdots \varrho_n^{s_n}$ by their expressions as furnished by (4), we have

$$(6) \qquad \alpha' \cdot \alpha'' \cdots \alpha^{(k)} = A_1\varrho_1 + A_2\varrho_2 + \cdots + A_n\varrho_n,$$

where

$$(7) \qquad A_i = \sum B_{s_1 s_2 \ldots s_n} C^{(i)}_{s_1 s_2 \ldots s_n},$$

the summation extending over all $s_1, s_2, \ldots, s_n$ whose sum is k.

The A_i, for whose computation a definite process is thus given, are rational integers. They will be used in the application whose consideration is the object of this paper.

3. *Ideals in R.* The *conductor of a ring* is an ideal f in $k(\theta)$ such that the product of any integer of $k(\theta)$ by f belongs to R.* By a *ring ideal* we shall understand an ideal in R as defined by Bachmann.† That is, an ideal $I^{(R)}$ of R is a set of integers of R such that the sum and difference of any two integers of the set belong to the set; the product of any integer of the set by any integer of R belongs to the set; and the greatest common divisor of f and the moduli thus defined is the ring R.

Let $I^{(R)}$ be any ideal of R, and let $\beta_1, \beta_2, \ldots, \beta_n$ be a fundamental system of $I^{(R)}$. Since the β_i belong to R, they can be represented by the form (2). If we write

$$(8) \qquad \beta_i = b_{i1}\varrho_1 + b_{i2}\varrho_2 + \cdots + b_{in}\varrho_n, \qquad (i = 1, 2, \ldots, n),$$

then the *norm of $I^{(R)}$* in R, which we shall denote by $N_R(I^{(R)})$, is the absolute value of the determinant $|b_{ij}|$.‡

If $\alpha = e_1\beta_1 + e_2\beta_2 + \cdots + e_n\beta_n$ is an integer in $I^{(R)}$, and if we apply (8), we have $\alpha = a_1\varrho_1 + a_2\varrho_2 + \cdots + a_n\varrho_n$, where

$$(9) \qquad a_i = b_{1i}e_1 + b_{2i}e_2 + \cdots + b_{ni}e_n, \qquad (i = 1, 2, \ldots, n),$$

whose matrix is the conjugate of that of (8).

In order to distinguish between ideals in R and ideals in $k(\theta)$, we shall speak of them as *ring ideals* and *field ideals*, respectively. Principal ring ideals will be designated by $[\lambda]$, where λ is an integer of R, and principal field ideals by $\{\lambda\}$, where λ is an integer of $k(\theta)$.

To every ideal $I^{(R)}$ of R there corresponds a field ideal I obtained by forming the product of $I^{(R)}$ and the unit ideal of $k(\theta)$; and if I is any ideal of $k(\theta)$ which is relatively prime to f, the numbers of I which belong to R constitute a ring ideal $I^{(R)}$ whose corresponding field ideal is I. The norm $N(I)$ of I is equal to the norm $N_R(I^{(R)})$ of $I^{(R)}$ in R.§ The index Δ of R is divisible by the conductor f of R.‖

* Bachmann, *Zahlentheorie,* p. 136.

† Bachmann, loc. cit., p. 363.

‡ Bachmann, loc. cit., chapter 2, p. 74.

§ Bachmann, loc. cit., chapter 9, No. 2.

‖ Bachmann, chapter 4, p. 136.

Two ideals $I_1^{(R)}$ and $I_2^{(R)}$ shall be called equivalent when R contains two integers α_1 and α_2 which are relatively prime to f, and $\alpha_2 I_1^{(R)} = \alpha_1 I_2^{(R)}$.* Equivalent ideals constitute a class.

For any given ring ideal $I^{(R)}$ there is an ideal $J^{(R)}$ such that the corresponding field ideal J is relatively prime to any given field ideal T and the product $I^{(R)} \cdot J^{(R)}$ is a principal ideal in R.

To prove this, we make use of the fact that an ideal $J_1^{(R)}$ exists, such that $J_1^{(R)}(I^{(R)} \cdot T_2^{(R)}) = [\lambda_1]$, a principal ideal in R.† Here T_2 is used to denote the product of the distinct prime factors of T which are relatively prime to f, and $T_2^{(R)}$ is used to denote the corresponding ring ideal.

Let T_1 be the product of the distinct prime factors of T which are divisors of f. Then $J_1^{(R)} \cdot T_2^{(R)}$ is relatively prime to T_1. For, since $J_1^{(R)}$ and $T_2^{(R)}$ are ideals in R, their product is an ideal in R. Hence this product is prime to f, and therefore also to T_1, which is a factor of f. There exists in $k(\theta)$ an ideal J_2 which is relatively prime to T_2, such that $J_2 \cdot I \cdot f = \{\lambda_2\}$.‡ Since λ_2 is divisible by f, it is an integer in R. I is the field ideal corresponding to the given ring ideal $I^{(R)}$.

Since λ_1 and λ_2 both belong to R, their sum $\lambda_1 + \lambda_2$ belongs to R, and since λ_1 and λ_2 are both divisible by $I^{(R)}$, there exists an ideal $J^{(R)}$ such that $I^{(R)} \cdot J^{(R)} = [\lambda_1 + \lambda_2]$.§

That λ_1 is divisible by $I^{(R)}$ is seen by its definition. Moreover, λ_2 is divisible by I and belongs to R and hence also to $I^{(R)}$; it is therefore divisible by $I^{(R)}$. Hence $\lambda_1 + \lambda_2$ is divisible by $I^{(R)}$.

The $J^{(R)}$ thus defined is such that the corresponding field ideal J is relatively prime to T. For, since $I^{(R)} \cdot J^{(R)} = [\lambda_1 + \lambda_2]$, by multiplying both members by the unit ideal of $k(\theta)$, we have $I \cdot J = \{\lambda_1 + \lambda_2\}$. Now λ_1 / I is relatively prime

* Bachmann uses the restricted equivalent in which $sgn N(\alpha_1) = sgn N(\alpha_2)$.

† Bachmann, loc. cit., p. 398.

‡ Bachmann, loc. cit., p. 221.

§ Bachmann, loc. cit., p. 369.

to T_1 and is divisible by T_2, and λ_2/I is relatively prime to T_2 and is divisible by T_1. Hence, if p is any prime factor of T and hence a factor of T_1 or T_2, either λ_1 or λ_2 is divisible by Ip, but not both. Hence their sum is not divisible by Ip, and therefore $\{\lambda_1+\lambda_2\}/I$ is not divisible by any prime factor of T. It follows that J is relatively prime to T. In the application to Diophantine equations this theorem will be used with $T=\{\Delta\}$.

4. *Decomposable Forms.* If $x_1\beta_1+x_2\beta_2+\cdots+x_n\beta_n$ is the fundamental form of the ideal $I^{(R)}$, then $N(x_1\beta_1+x_2\beta_2+\cdots+x_n\beta_n)$ is a form of degree n in the n variables $x_1, x_2, \ldots, x_n$, with rational integral coefficients. The highest common factor of the coefficient of this form is the norm of the ideal $I^{(R)}$ in R. Hence

$$(10)\quad N(x_1\beta_1+x_2\beta_2+\cdots+x_n\beta_n)=N_R(I^{(R)})\,F(x_1,x_2,\ldots,x_n),$$

where $F(x_1, x_2, \ldots, x_n)$ is a unit form decomposable in R.*

The following theorem is a modified form of one given by Bachmann.† The modifications are made so as to apply to ideals in R, and also for the equivalence as we have defined it.

If $J^{(R)}$ is any ideal of R and $F(x_1, x_2, \ldots, x_n)$ is a unit form obtained as above from an ideal $I^{(R)}$ of the class reciprocal to that of $J^{(R)}$, then there exist rational integers e_1, $e_2, \ldots, e_n$, such that $N_R(J^{(R)}) = |F(e_1, e_2, \ldots, e_n)|$; and, conversely, any rational integer $F(e_1, e_2, \ldots, e_n)$ represented by the decomposable form $F(x_1, x_2, \ldots, x_n)$ is in absolute value the norm of an ideal of the class reciprocal to that of $I^{(R)}$ provided $e_1\beta_1+e_2\beta_2+\cdots+e_n\beta_n$ is prime to f.

Let $\beta_1, \beta_2, \ldots, \beta_n$ be the fundamental system of $I^{(R)}$ from which the form $F(x_1, x_2, \ldots, x_n)$ is obtained, and let $I^{(R)}J^{(R)} = [\gamma]$. Then $\gamma = e_1\beta_1+e_2\beta_2+\cdots+e_n\beta_n$, and

$$|N(\gamma)| = N_R(I^{(R)})\cdot N_R(J^{(R)}) = N(e_1\beta_1+e_2\beta_2+\cdots+e_n\beta_n)$$
$$= N_R(I^{(R)})\,|F(e_1, e_2, \ldots, e_n)|,$$

and hence

$$N_R(J^{(R)}) = |F(e_1, e_2, \ldots, e_n)|.$$

* Bachmann, loc. cit., chapter 10, No. 6.

† Bachmann, loc. cit., p. 429.

Conversely, if $F(e_1, e_2, \ldots, e_n)$ is any rational integer represented by $F(x_1, x_2, \ldots, x_n)$ corresponding to the ring ideal $I^{(R)}$, then

$$N_R(I^{(R)})F(e_1, e_2, \ldots, e_n) = N(e_1\beta_1 + e_2\beta_2 + \cdots + e_n\beta_n).$$

But if $e_1\beta_1 + e_2\beta_2 + \cdots + e_n\beta_n$ is prime to f, $[e_1\beta_1 + e_2\beta_2 + \cdots + e_n\beta_n]$ is a principal ideal in R; and, since it is divisible by $I^{(R)}$, there exists in the reciprocal class an ideal $J_1^{(R)}$ such that

$$J_1^{(R)} \cdot I^{(R)} = [e_1\beta_1 + e_2\beta_2 + \cdots + e_n\beta_n].$$

Hence we may write

$$|N(e_1\beta_1 + \cdots + e_n\beta_n)| = N_R(J_1^{(R)})\, N_R(I^{(R)}),$$

whence it follows that

$$N_R(J_1^{(R)}) = F(e_1, e_2, \ldots, e_n).$$

If $e_1\beta_1 + e_2\beta_2 + \cdots + e_n\beta_n$ is not prime to F and if I is the field ideal corresponding to $I^{(R)}$, then

$$\{\gamma\} = \{e_1\beta_1 + e_2\beta_2 + \cdots + e_n\beta_n\}$$

is divisible by I, and $\{\gamma\}/I = J_1$ is a field ideal which is not relatively prime to f. The method used above will show that the absolute value of $F(e_1, e_2, \ldots, e_n)$ is the norm of J_1.

5. *Application to Diophantine Equations.* We shall now turn our attention to the application of the foregoing facts regarding rings and ring ideals to the solution in rational integers $\xi_1, \xi_2, \ldots, \xi_n;\ u_1, u_2, \ldots, u_{k-2}$ of the equation

$$(11) \qquad N(\xi_1\varrho_1 + \xi_2\varrho_2 + \cdots + \xi_n\varrho_n) = u_1 \cdot u_2 \cdots u_{k-2},$$

where as before $\varrho_1, \varrho_2, \ldots, \varrho_n$ is a fundamental system of any ring R in $k(\theta)$.

Let us suppose that we have a set of integers satisfying (11). Since $\varrho_1, \varrho_2, \ldots, \varrho_n$ is a fundamental system of R, $\gamma = \xi_1\varrho_1 + \xi_2\varrho_2 + \cdots + \xi_n\varrho_n$ is an integer of $k(\theta)$. We shall suppose it resolved into its ideal prime factors. There are s distinct factors. We shall denote them by $p_1, p_2, \ldots, p_s$. Let us suppose that the first s_1 of these are relatively prime to f. Let $p_1^{\lambda_{11}}$ be the highest power of p_1 which is a factor of γ and whose norm is a factor of u_1; $p_1^{\lambda_{12}}$ the highest power of p_1 which is a factor of $\gamma/p_1^{\lambda_{11}}$ and whose norm is a factor of u_2; $p_1^{\lambda_{13}}$ the highest power of p_1 which is a divisor of $\gamma/p_1^{\lambda_{11}+\lambda_{12}}$ and whose norm is a divisor of u_3; and so on, until finally $p_1^{\lambda_{1k-2}}$ is the highest power of p_1 which is a divisor of $\gamma/p_1^{\lambda_{11}+\lambda_{12}+\cdots+\lambda_{1k-3}}$ and whose norm is a factor of u_{k-2}.

We next consider the prime ideal p_2 in the same way, and we let $p_2^{\lambda_{21}}$ be the highest power of p_2 which is a divisor of γ and whose norm is a divisor of $u_1/N(p_1^{\lambda_{11}})$; $p_2^{\lambda_{22}}$ the highest power of p_2 which is a divisor of $\gamma/p_2^{\lambda_{21}}$ and whose norm is a divisor of $u_2/N(p_1^{\lambda_{12}})$; and we continue in this way until finally $p_{s_1}^{\lambda_{s_1k-2}}$ is the highest power of p_{s_1} which is a divisor of $\gamma/p_{s_1}^{\lambda_{s_11}+\lambda_{s_12}+\cdots+\lambda_{s_1k-3}}$ and whose norm is a divisor of $u_{k-2}/N(p_1^{\lambda_{1k-2}}\cdot p_2^{\lambda_{2k-2}}\cdots p_{s-1}^{\lambda_{s-1\,k-2}})$.

We shall now write

$$P_i = p_1^{\lambda_{1i}}\cdot p_2^{\lambda_{2i}}\cdots p_{s_1}^{\lambda_{s_1i}}, \qquad (i = 1, 2, \ldots, k—2).$$

From the construction of the P_i, we see that γ is divisible by the product $P_1\cdot P_2\cdots P_{k-2}$, and that u_i is divisible by $N(P_i)$. We shall therefore write

$$Q = \frac{\{\gamma\}}{P_1\cdot P_2\cdots P_{k-2}},$$

and

$$u_i = \mu_i\cdot N(P_i).$$

Let us next write $Q = P_{k-1}\cdot P_k$ where P_k is the largest factor of Q all of whose prime divisors are divisors of f. We then have

$$\{\gamma\} = P_1\cdot P_2\cdots P_k,$$

where $P_1, P_2, \ldots, P_{k-1}$ are prime to f, and P_k contains no prime factor excepting factors of f. By (11), we have then

$$\begin{aligned} |N(\gamma)| &= N(P_1)\cdot N(P_2)\cdots N(P_k) = |u_1\cdot u_2\cdots u_{k-2}| \\ &= |\mu_1\cdot\mu_2\cdots\mu_{k-2}|\, N(P_1)\cdot N(P_2)\cdots N(P_{k-2}). \end{aligned}$$

Hence

$$N(P_{k-1})\cdot N(P_k) = |\mu_1\cdot\mu_2\cdots\mu_{k-2}|.$$

Let us separate each μ_i into two factors μ_i' and μ_i'' such that

$$\begin{aligned} N(P_{k-1}) &= |\mu_1'\cdot\mu_2'\cdots\mu_{k-2}'|, \\ N(P_k) &= |\mu_1''\cdot\mu_2''\cdots\mu_{k-2}''|. \end{aligned}$$

Since the $P_1, P_2, \ldots, P_{k-1}$, are all relatively prime to f, to each P_i, $(i<k)$, there corresponds a ring ideal whose norm in the ring is equal to the norm of P_i in $k(\theta)$. Let $P_i^{(R)}$ be the ring ideal corresponding to P_i. Let $I_i^{(R)}$ be an ideal from the reciprocal class. According to § 3, $I_i^{(R)}$ can be so chosen that the corresponding field ideal I_i is relatively prime to $\{\varDelta\}$. We shall suppose that $I_i^{(R)}$ has been so chosen. Let $\beta_1^{(i)}, \beta_2^{(i)}, \ldots, \beta_n^{(i)}$ be a fundamental system of $I_i^{(R)}$, and let $F_i(x_1, x_2, \ldots, x_n)$ be the corresponding decomposable form. Then, by § 4, we have

$$N_R(P_i^{(R)}) = N(P_i) = \left| F_i(e_1^{(i)}, e_2^{(i)}, \ldots, e_n^{(i)}) \right|,$$

and hence

$$(12) \qquad u_i = \varepsilon_i \cdot \mu_i' \cdot \mu_i'' \, F_i(e_1^{(i)}, e_2^{(i)}, \ldots, e_n^{(i)}), \qquad (i = 1, 2, \ldots, k-2),$$

where ε_i is 1 or -1. Since $I_i^{(R)}$ and $P_i^{(R)}$ belong to reciprocal classes, $I_i^{(R)} \cdot P_i^{(R)} = [\alpha^{(i)}]$. Hence, since $[\alpha^{(i)}]$ is divisible by $I_i^{(R)}$, we have

$$\begin{aligned} \alpha^{(i)} &= e_1^{(i)} \beta_1^{(i)} + e_2^{(i)} \beta_2^{(i)} + \cdots + e_n^{(i)} \beta_n^{(i)} \\ &= a_{1i} \varrho_1 + a_{2i} \varrho_2 + \cdots + a_{ni} \varrho_n, \qquad (i = 1, 2, \ldots, k-1). \end{aligned}$$

Since P_k contains no prime factors except such as are factors of f, let us suppose that J is the smallest field ideal (i. e., the field ideal containing the fewest prime factors) whose product with P_k is divisible by f, and let M_1 be the smallest rational integer which is divisible by J. Let $M_2 = N(I)$, where $I = I_1 \cdot I_2 \cdots I_{k-1}$.

The ideal I is relatively prime to the principal ideal $\{\varDelta\}$. Hence, since $\varDelta$ is a rational integer, M_2 and $\varDelta$ are relatively prime. Since M_2 is divisible by I, we can choose I_k such that $I \cdot I_k = \{M_2\}$, and I_k is then relatively prime to $\varDelta$, and hence also to f, which is a divisor of $\varDelta$.

Since $\{\gamma\} = P_1 \cdot P_2 \cdots P_k$, P_k belongs to the class reciprocal to that of $P_1 \cdot P_2 \cdots P_{k-1}$. But I belongs to the class reciprocal to that of $P_1 \cdot P_2 \cdots P_{k-1}$. Hence P_k and I belong to the same class, and P_k and I_k belong to reciprocal classes. Therefore $P_k I_k = \{\bar{\alpha}^{(k)}\}$.

Let us now write $\bar{\alpha} = \alpha' \cdot \alpha'' \cdots \alpha^{(k-1)} \cdot \bar{\alpha}^{(k)} \cdot M_1$. Since $\bar{\alpha}^{(k)} M_1$ is divisible by JP_k, it is divisible by f, and hence $\bar{\alpha}$ is an integer in R. In fact, $\bar{\alpha}^{(k)} \cdot M_1$ belongs to R, and we may therefore write

$$\bar{\alpha}^{(k)} \cdot M_1 = \bar{a}_{1k}\varrho_1 + \bar{a}_{2k}\varrho_2 + \cdots + \bar{a}_{nk}\varrho_n.$$

Moreover

$$\{\bar{\alpha}\} = P_1 \cdot P_2 \cdots P_k \cdot I_1 \cdot I_2 \cdots I_k \cdot M_1 = \{\gamma M_2 M_1\},$$

and hence $\bar{\alpha}$ and $\gamma M_1 M_2$ differ only by a factor which is a unit in $k(\theta)$. Then let us write $\bar{\alpha} = E\gamma \cdot M_1 \cdot M_2$. But since $\bar{\alpha}^{(k)} M_1$ is divisible by f, $E \cdot \bar{\alpha}^{(k)} \cdot M_1$ is also divisible by f, and hence belongs to R. Then, if we put $E\bar{\alpha}^{(k)} = \alpha^{(k)}$, we may write

$$M_1 E \bar{\alpha}^{(k)} = M_1 \alpha^{(k)} = a_{1k}\varrho_1 + a_{2k}\varrho_2 + \cdots + a_{nk}\varrho_n;$$

and since $\{\bar{\alpha}^{(k)}\} = \{\alpha^{(k)}\}$, we have $P_k I_k = \{\alpha^{(k)}\}$, and

$$\alpha = \alpha' \cdot \alpha'' \cdots \alpha^{(k)} M_1 = \gamma \cdot M_1 \cdot M_2.$$

We therefore have

$$\begin{aligned} M_1 M_2 \gamma &= M_1 M_2 (\xi_1 \varrho_1 + \xi_2 \varrho_2 + \cdots + \xi_n \varrho_n) \\ &= \prod_{i=1}^{k} (a_{1i}\varrho_1 + a_{2i}\varrho_2 + \cdots + a_{ni}\varrho_n), \end{aligned}$$

and using the notations of § 2, we have

$$\xi_i = \frac{A_i}{M_1 \cdot M_2}, \qquad (i = 1, 2, \ldots, n). \tag{13}$$

Here the A_i are polynomials in the a_{ji}, $(j = 1, 2, \ldots, n;\ i = 1, 2, \ldots, k)$, which upon application of (9) to the elements standing in the first $k-2$ rows of the matrix of § 2 as they occur in the A_i, gives an expression for the ξ_i in terms of the parameters $e_j^{(i)}$ which occur in the expressions for u_i, and the elements of the last two rows of the matrix which are implicitely involved in the u_i in the factors μ_i' and μ_i''.

We have thus by means of (12) and (13) obtained a general form for the solution of (11). We shall next see that all such expressions, when the parameters are given rational integral values, constitute a solution of (11).

Substituting for $\xi_1, \xi_2, \ldots, \xi_n$; $u_1, u_2, \ldots, u_{k-2}$ their values as given by (12) and (13) in (11), we have the equation

$$(14)\qquad \frac{N(A_1\varrho_1+\cdots+A_n\varrho_n)}{M_1^n\cdot M_2^n}=\prod_{i=1}^{k-2}\varepsilon_i\mu_i'\mu_i''F_i(e_1^{(i)},e_2^{(i)},\ldots,e_n^{(i)}).$$

Since

$M_2=I\cdot I_k,\ N(I_i)=N_R(I_i^{(R)}),\ |\mu_1'\cdot\mu_2'\cdots\mu_{k-2}'|=N_R(P_{k-1}^{(R)}),$

and $P_{k-1}^{(R)}\cdot I_{k-1}^{(R)}=[\alpha^{(k-1)}]$, a principal ideal in R, we can write (14) in the form

$$(15)\qquad \begin{aligned} &N(A_1\varrho_1+A_2\varrho_2+\cdots+A_n\varrho_n)\\ &=M_1^nM_2^{n-1}N_R(I_{k-1}^{(R)})\mu_1'\cdot\mu_2'\cdots\mu_{k-2}'\prod_{i=1}^{k-2}\varepsilon_i\mu_i''N_R(I_i^{(R)})\\ &\qquad\times F_i(e_1^{(i)},\ldots,e_n^{(i)}).\end{aligned}$$

But

$$\begin{aligned} N_R(I_i^{(R)})F_i(e_1^{(i)},e_2^{(i)},\ldots,e_n^{(i)})&=N(e_1^{(i)}\beta_1^{(i)}+\cdots+e_n^{(i)}\beta_n^{(i)})\\ &=N(a_{1i}\varrho_1+a_{2i}\varrho_2+\cdots+a_{ni}\varrho_n).\end{aligned}$$

Also

$$\begin{aligned} N_R(I_{k-1}^{(R)})\cdot|\mu_1'\cdot\mu_2'\cdots\mu_{k-2}'|&=N_R(I_{k-1}^{(R)})N_R(P_{k-1}^{(R)})\\ &=N\{\alpha^{(k-1)}\}=\varepsilon^{k-1}N(\alpha^{(k-1)})\\ &=\varepsilon_{k-1}N(a_{1k-1}\varrho_1+a_{2k-1}\varrho_2+\cdots+a_{nk-1}\varrho_n).\end{aligned}$$

Let us suppose that the signs of $\mu_1',\mu_2',\ldots,\mu_{k-2}'$ have been so chosen that the sign of their product is the same as the sign of $N(\alpha^{(k-1)})$ and hence $\varepsilon_{k-1}=+1$. If we now put $\varepsilon=\varepsilon_1\cdot\varepsilon_2\cdots\varepsilon_{k-2}$, we may write (15) in the form

$$(16)\qquad \begin{aligned} &N(A_1\varrho_1+A_2\varrho_2+\cdots+A_n\varrho_n)\\ &=\varepsilon M_1^nM_2^{n-1}\mu_1''\cdot\mu_2''\cdots\mu_{k-2}''\prod_{i=1}^{k-1}N(a_{1i}\varrho_1+\cdots+a_{ni}\varrho_n).\end{aligned}$$

Since $M_2=I\cdot I_k=N(I)$, we have

$$M_2^n=N(I)N(I_k)=M_2N(I_k),$$

and hence $M_2^{n-1}=N(I_k)$. Also $|\mu_1''\cdot\mu_2''\cdots\mu_{k-2}''|=N(P_k)$, and therefore

$$(17)\qquad \begin{aligned} M_1^nM_2^{n-1}|\mu_1''\cdot\mu_2''\cdots\mu_{k-2}''|&=M_1^nN(I_k\cdot P_k)=N\{M_1\alpha^{(k)}\}\\ &=N\{a_{1k}\varrho_1+a_{2k}\varrho_2+\cdots+a_{nk}\varrho_n\}.\end{aligned}$$

For, since $M_1\alpha^{(k)}$ is divisible by f, it belongs to R. As above, we shall now affix signs to the μ_i'' so that the sign of their product is the same as the sign of $N(\alpha^{(k)})$. Then we have

$$M_1^n \cdot M_2^{n-1} \mu_1'' \cdot \mu_2'' \cdots \mu_{k-2}'' = N(a_{1k}\varrho_1 + a_{2k}\varrho_2 + \cdots + a_{nk}\varrho_n).$$

We may now write (16) in the form

$$N(A_1\varrho_1 + A_2\varrho_2 + \cdots + A_n\varrho_n) = \varepsilon \prod_{i=1}^{k} N(a_{1i}\varrho_1 + a_{2i}\varrho_2 + \cdots + a_{ni}\varrho_n),$$

which, by § 1, is seen to be an identity if $\varepsilon = +1$.

Hence, with the signs of the μ_i' and μ_i'' properly chosen, and ε_i so chosen that their product is $+1$, all numbers obtained by (12) and (13) are solutions of (11). We observe, however, that the expressions for $\xi_1, \xi_2, \ldots, \xi_n$ are fractional in form. Hence we must next determine under what conditions they are integral, that is, we must determine what conditions must be imposed on the μ_i' and μ_i'' in order that the solutions shall be integral, or in other words, that γ shall belong to R.

From the development, it follows that, for

$$\gamma = \frac{A_1\varrho_1 + A_2\varrho_2 + \cdots + A_n\varrho_n}{M_1M_2},$$

$M_1 \cdot M_2 \cdot \gamma$ is an integer in R and

$$\{\gamma\} = \left\{\frac{A_1\varrho_1 + A_2\varrho_2 + \cdots + A_n\varrho_n}{M_1M_2}\right\} = P_1 \cdot P_2 \cdots P_k$$

is a principal ideal of the field. Since the product of any integer of the field by Δ is an integer of R, we know that

$$\frac{A_1\Delta\varrho_1 + A_2\Delta\varrho_2 + \cdots + A_n\Delta\varrho_n}{M_1M_2}$$

is an integer of R. Hence it is equal to $C_1\varrho_1 + C_2\varrho_2 + \cdots + C_n\varrho_n$, where $C_1, C_2, \ldots, C_n$ are rational integers. But the representation by the fundamental system is unique; hence

$$\frac{A_i\Delta}{M_1M_2} = C_i.$$

Since M_2 is relatively prime to Δ, this says that A_i is divisible by M_2; hence (13) will not give fractions with factors of M_2 in the denominator.

We have defined J as the smallest ideal whose product with P_k is divisible by f, and M_1 as the smallest rational integer divisible by J. Let $M_1 = M_1' \cdot M_1''$, where M_1' is the smallest factor of M_1 such that $M_1' P_k I_k = \{\gamma^{(k)}\}$, when $\gamma^{(k)}$ is an integer of R. If we then choose $\alpha^{(k)}$ in $P_k \cdot I_k = \{\alpha^{(k)}\}$ such that $M_1 \alpha^{(k)} = M_1'' \gamma^{(k)}$, which is always possible since

$$M_1''\{\gamma^{(k)}\} = M_1 P_k I_k = M_1' M_1'' \{\alpha^{(k)}\},$$

we see that the $a_{1k}, a_{2k}, \ldots, a_{nk}$ are all multiples of M_1'' since $\gamma^{(k)}$ belongs to R. We thus see that the A_i are all divisible by M_1'' and only factors of M_1' can occur in the denominators of the numbers furnished by (13).

In the first part of this article, we have seen that all integral solutions of (11) can be expressed by (12) and (13). In the proof as given, for $i < k$ the

$$e_1^{(i)}\beta_1^{(i)} + e_2^{(i)}\beta_2^{(i)} + \cdots + e_n^{(i)}\beta_n^{(i)} = a_{1i}\varrho_1 + a_{2i}\varrho_2 + \cdots + a_{ni}\varrho_n$$

were all relatively prime to f. Hence the product

$$\prod = \prod_{i=1}^{k-1} (a_{1i}\varrho_1 + a_{2i}\varrho_2 + \cdots + a_{ni}\varrho_n)$$

is also relatively prime to f. The integer $\prod$ belongs to R. Hence if

$$(a_{1k}\varrho_1 + a_{2k}\varrho_2 + \cdots + a_{nk}\varrho_n) \prod = \prod_{i=1}^{k} (a_{1i}\varrho_1 + a_{2i}\varrho_2 + \ldots + a_{ni}\varrho_n)$$

should have all its coefficients, when it is written as a linear function of $\varrho_1, \varrho_2, \ldots, \varrho_n$, divisible by some factor $M_1^{(3)}$ of $M_1' = M_1^{(3)} \cdot M_1^{(4)}$ it would follow that

$$\frac{a_{1k}\varrho_1 + a_{2k}\varrho_2 + \cdots + a_{nk}\varrho_n}{M_1' \cdot M_1''} M_1^{(4)} \cdot \prod$$

would be an integer of R.

Hence the product of

$$\frac{a_{1k}\varrho_1 + a_{2k}\varrho_2 + \cdots + a_{nk}\varrho_n}{M_1' \cdot M_1''} M_1^{(4)}$$

by $\prod$, or by any integer divisible by f, would be an integer of R. But $\prod$ belongs to R, and the principal ideal $[\prod]$

is relatively prime to f. Hence there exists an integer C in R and an integer D in f such that $C \cdot \prod + D = 1$.*

Since $C\prod$ belongs to R, the products of

$$\frac{a_{1k}\varrho_1 + a_{2k}\varrho_2 + \cdots + a_{nk}\varrho_k}{M_1' \cdot M_1''} M_1^{(4)}$$

by $C\prod$ and by D, and hence also the sum of these products, belong to R. Therefore

$$\frac{a_{1k}\varrho_1 + a_{2k}\varrho_2 + \cdots + a_{nk}\varrho_n}{M_1' \cdot M_1''} M_1^{(4)}$$

is an integer in R. But $\{\alpha^{(k)}\} = P_k I_k$, and

$$M_1' \cdot M_1'' P_k I_k = \{a_{1k}\varrho_1 + a_{2k}\varrho_2 + \cdots + a_{nk}\varrho_n\}.$$

Hence

$$M_1^{(4)} P_k I_k = \left\{\frac{a_{1k}\varrho_1 + a_{2k}\varrho_2 + \cdots + a_{nk}\varrho_n}{M_1' \cdot M_1''} M_1^{(4)}\right\},$$

where the integer determining the principal ideal belongs to R. But we have assumed that M_1' is the smallest factor of M_1 such that when $M_1' P_k I_k = \{\gamma^{(k)}\}$ the $\gamma^{(k)}$ belongs to R; hence $M_1^{(4)} = M_1'$, i. e., $M_1^{(3)} = 1$.

Therefore M_1' will always occur as a denominator in the numbers furnished by (13), and integral solutions are possible only when $M_1' = 1$. Consequently, in order to have integral solutions, $\alpha^{(k)}$ must be an integer of R.

We have seen that $a_{1k}, a_{2k}, \ldots, a_{nk}$ are all divisible by M_1''. Hence if we put $a_{ik}/M_1'' = C_{ik}$ we shall have

$$\gamma^{(k)} = C_{1k}\varrho_1 + C_{2k}\varrho_2 + \cdots + C_{nk}\varrho_n.$$

The matrix obtained from m in § 2 by replacing the a_{ik} by the C_{ik}, $(i = 1, 2, \ldots, n)$, shall be denoted by m'.

From the theory of the correspondence between ideals and decomposable forms, we know that to a class of ideals corresponds a class of forms. Any form of the class can be obtained by proper choice of the base of the ideal, from any ideal of the corresponding class of ideals by the method of § 4. Moreover, the numbers represented by any form of the class can be represented by every form of the class.

Let γ be any integer of R. Suppose that the principal field ideal $\{\gamma\}$ is separated into the product $T \cdot P_k$ of two field

* Bachmann, loc. cit., p. 367.

ideals such that T is relatively prime to f, and that P_k contains no prime factors except such as are divisors of f. Let $T^{(R)}$ be the ring ideal corresponding to T. From the reciprocal class in R, select an ideal $I^{(R)}$ whose corresponding field ideal I is relatively prime to $\{\Delta\}$. Let $N(I) = M_2$. Then M_2 is relatively prime to Δ, and hence also to f, which is a divisor of Δ. Therefore $I_k = \{M_2\}/I$ is relatively prime to f, and the corresponding ring ideal $I_k^{(R)}$ belongs to the class reciprocal to that of $I^{(R)}$.

Since $I^{(R)}$ and $T^{(R)}$ belong to reciprocal classes in R, we have $I^{(R)}T^{(R)} = [\alpha]$. Multiplying both members of this equation by the unit ideal of $k(\theta)$, we have $I \cdot T = \{\alpha\}$. It is easily seen that I_k and P_k belong to reciprocal classes. Hence $I_k \cdot P_k = \{\gamma^{(k)}\}$. We shall next see that the integer $\gamma^{(k)}$ belongs to R.

We have $T \cdot P_k = \{\gamma\}$ and γ was chosen an integer of R. Since M_2 is a rational integer, $M_2\gamma$ belongs to R. Since $I^{(R)}$ was chosen from the class reciprocal to that of $T^{(R)}$ in R, α belongs to R and is relatively prime to f. We may write

$$I_k P_k = \frac{\{M_2\}}{I} \cdot P_k = \frac{\{M_2\} T \cdot P_k}{I \cdot T} = \left\{\frac{M_2\gamma}{\alpha}\right\} = \{\gamma^{(k)}\},$$

and hence we may write $\gamma^{(k)} = M_2\gamma/\alpha$. Therefore $\gamma^{(k)} \cdot \alpha$ belongs to R; and, if a is any integer of $[\alpha]$, $\gamma^{(k)} \cdot a$ belongs to R. Also if b is any integer of f, $\gamma^{(k)} \cdot b$ belongs to R and therefore $\gamma^{(k)}(a+b)$ belongs to R. But since $[\alpha]$ is relatively prime to f, a and b may be so chosen that $a + b = 1$. Hence $\gamma^{(k)}$ belongs to R.

We may now sum up the result of the investigation as follows. Let $k(\theta)$ be any algebraic number field of degree n, and $\varrho_1, \varrho_2, \ldots, \varrho_n$ a fundamental system of a ring R whose conductor is f and index Δ. Select any integer γ from R and separate the principal ideal $\{\gamma\}$ into two factors $T \cdot P_k$, where T is relatively prime to the conductor f, and where P_k contains no prime factors except divisors of f. Let $T^{(R)}$ be the ring ideal corresponding to T, and $I^{(R)}$ an ideal from the reciprocal class in R whose corresponding field ideal I is relatively prime to $\{\Delta\}$. Let $M_2 = N(I)$, and $I_k = M_2/I$.

Then

$$I_k \cdot P_k = \{\gamma^{(k)}\} = \{C_{1k}\varrho_1 + C_{2k}\varrho_2 + \cdots + C_{nk}\varrho_n\},$$

since, as we have seen above, $\gamma^{(k)}$ belongs to R.

Select $k-2$ rational integers $\mu_1'', \mu_2'', \ldots, \mu_{k-2}''$, such that their product has the same sign as $N(\gamma^{(k)})$, and an absolute value equal to $N(P_k)$.

Next select $k-1$ ideals $I_1, I_2, \ldots, I_{k-1}$ whose product is I. As before, let $I_i^{(R)}$ be the ring ideal corresponding to I_i. Let $F_i(x_1, x_2, \ldots, x_n)$, $(i = 1, 2, \ldots, k-2)$, be the decomposable forms corresponding to the ideals $I_i^{(R)}$, $(i = 1, 2, \ldots, k-2)$. Choose an ideal $P_{k-1}^{(R)}$ from the class reciprocal to that of $I_{k-1}^{(R)}$ and let

$$P_{k-1}^{(R)} \cdot I_{k-1}^{(R)} = \left[\alpha^{(k-1)}\right] = [a_{1k-1}\varrho_1 + a_{2k-1}\varrho_2 + \cdots + a_{nk-1}\varrho_n].$$

Next select $k-2$ rational integers $\mu_1, \mu_2', \ldots, \mu_{k-2}'$ whose product has the sign of $N(\alpha^{(k-1)})$ and the absolute value $N(P_{k-1})$. Then for rational integral $e_j^{(i)}$, $(i = 1, 2, \ldots, k-2;$ $j = 1, 2, \ldots, n)$, and $\varepsilon_i = +1$ or -1, such that $\varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_{k-2} = +1$ the numbers

$$u_i = \varepsilon_i \mu_i' \cdot \mu_i'' F_i(e_1^{(i)} \cdot e_2^{(i)} \cdots e_n^{(i)}), \qquad (i = 1, 2, \cdots, k-2),$$

$$\xi_i = \frac{A_i}{M_2}, \qquad (i = 1, 2, \cdots, n),$$

constitute a solution of the equation

$$N(\xi_1\varrho_1 + \xi_2\varrho_2 + \cdots + \xi_n\varrho_n) = u_1 \cdot u_2 \cdots u_{k-2}.$$

The A_i are computed as in § 2 from the matrix

$$m' = \begin{Vmatrix} a_{11}, & a_{21}, & \ldots, & a_{n1} \\ a_{12}, & a_{22}, & \ldots, & a_{n2} \\ \cdot & \cdot & \cdot & \cdot \\ a_{1k-1}, & a_{2k-1}, & \ldots, & a_{nk-1} \\ c_{1k}, & c_{2k}, & \ldots, & c_{nk} \end{Vmatrix}$$

when the a_{ij} in the first $k-2$ rows of the matrix are obtained from the $e_j^{(i)}$ by means of $k-2$ sets of equations such as (9), one set for each of the ideals $I_i^{(R)}$, $(i = 1, 2, \ldots, k-2)$.

By the same method, all solutions of the given Diophantine equation may be obtained.

THE UNIVERSITY OF ILLINOIS