A QUADRATIC ALGEBRA AND ITS APPLICATION TO A PROBLEM IN DIOPHANTINE ANALYSIS*

BY G. E. WAHLIN

1. *Introduction.* Dickson† has studied the problem of the application of algebras in the determination of the solutions of certain Diophantine equations. In the following pages I shall define a system which is a generalization of those defined by Clifford‡ and Lipschitz.§

The algebra as here defined is sufficient for the application which I wish to make. By further restrictions on the basal elements we can define an algebra which is intimately connected with the theory of quadratic forms. This I hope to show in a later paper.

2. *Quadratic Extensions of a Field.* We shall assume a certain fundamental field K on which we shall construct an algebra by the adjunction of certain new elements. Let us first consider a quadratic equation

$$x^2 - ax + b = 0, \tag{1}$$

whose coefficients are numbers of K. We shall denote by r a root of this equation. This root r is so defined that $r^2 - ar + b = 0$ but it does not satisfy a linear equation with coefficients in K, even in the case when the equation (1) is reducible in this field. If $b = 0$, a simple linear transformation will transform (1) into an equation in which the last term is not zero and we shall therefore assume that all the quadratic equations with which we are concerned are such that the term which does not involve x is different from zero.

---

* Presented to the Society, April 10, 1925.

† *Algebras and their Arithmetics*, University of Chicago Press.

‡ American Journal, vol. 1, p. 350.

§ Comptes Rendus, vol. 91. pp. 619–660.
Bulletin de la Société de France, (2), vol. 11, p. 115.

The multiplication of r by any number of K shall be commutative and in any product of r and numbers of K multiplication shall be associative. We shall also assume the distributive law.

By a quadratic extension of K we mean the set of all elements of the form $mr+n$ where m and n are numbers of K.

Since $r^2=ar-b$ any power of r is equal to a linear function of r and hence it is easily seen that the sum, difference or product of any two elements of the quadratic extension of K belong to the same. Moreover, since r does not satisfy a linear equation in K, $mr+n$ is zero when and only when m and n are both zero.

In the case when the equation (1) is irreducible the quadratic extension of K is closed also with respect to division and is a field which is isomorphic with the ordinary algebraic number field defined by the equation. We shall call this a quadratic extension of the first type.

When the equation (1) is reducible in K we may write $x^2-ax+b=(x-\rho_1)(x-\rho_2)$. Due to the assumption of the commutative and distributive laws we see that this equality is true when we replace x by r and hence

$$(r-\rho_1)(r-\rho_2)=r^2-ar+b=0.$$

But $r-\rho_1\neq 0$ and $r-\rho_2\neq 0$ since r does not satisfy an equation of the first degree. Hence $r-\rho_1$ and $r-\rho_2$ are proper divisors of zero and a unique and universal division process is not possible. We shall call this a quadratic extension of the second type.

It is easily seen that in either of the two types of quadratic extensions the multiplication is associative and commutative.

The element r as above defined cannot satisfy more than one quadratic equation in K, for if we have $r^2-ar+b=0$, and also $r^2-a'r+b'=0$, we find $(a'-a)r-(b'-b)=0$, which is impossible unless $a'=a$ and $b'=b$.

3. *Conjugate Roots.* Let us next consider the element $a-r$ and substitute it for x in (1). This gives

$$(a - r)^2 - a(a - r) + b = a^2 - 2ar + r^2 - a^2 + ar + b$$
$$= r^2 - ar + b = 0.$$

Hence $a-r$ is also a solution of (1). We shall write $r' = a-r$ and speak of r and r' as a pair of conjugate roots of (1).

From the definition of r' it follows that $r+r' = a$ and $rr' = r'r = (a-r)r = ar - r^2 = b$. The sum $S(r) = r+r'$ is called the *trace* of r, and the product $rr' = N(r)$ is called the *norm* of r.

4. *An Algebra of Order Four.* Let us consider a ternary quadratic form

$$Q(x, y_1, y_2) = x^2 + b_1 y_1^2 + b_2 y_2^2 + a_1 x y_1 + a_2 x y_2 + c y_1 y_2,$$

and let us suppose that r_1 and r_2 are a pair of elements such that with another, associated, pair of elements r_1' and r_2' and a properly defined multiplication

$$(2) \quad \begin{cases} Q(x, y_1, y_2) = (x + r_1 y_1 + r_2 y_2)(x + r_1' y_1 + r_2' y_2) \\ \qquad = x^2 + r_1 r_1' y_1^2 + r_2 r_2' y_2^2 + (r_1 + r_1')xy_1 \\ + (r_2 + r_2')xy_2 + (r_1 r_2' + r_2 r_1')y_1 y_2. \end{cases}$$

Then

$$(3) \quad r_1 + r_1' = a_1, \quad r_2 + r_2' = a_2, \quad r_1 r_1' = b_1, \quad r_2 r_2' = b_2,$$
$$r_1 r_2' + r_2 r_1' = c.$$

We shall assume that the coefficients a_1, a_2, b_1, b_2, c belong to the field K and that each of the elements r_1 and r_2 has a multiplication with the elements of K subject to the assumptions of the preceding sections.

From (2) we have

$$Q(x, -1, 0) = x^2 - a_1 x + b_1 = (x - r_1)(x - r_1')$$

and hence r_1 and r_1' are a pair of conjugate roots of the equation $Q(x, -1, 0) = 0$. In the same way, r_2 and r_2' are a pair of conjugate roots of $Q(x, 0, -1) = 0$, and $r_1 + r_2$ and $r_1' + r_2'$

a pair of conjugate roots of $Q(x, -1, -1)=0$. Hence we have the following relations:

$$r_1^2 = a_1r_1 - b_1, \tag{4}$$

$$r_2^2 = a_2r_2 - b_2, \tag{5}$$

$$(r_1 + r_2)^2 = (a_1 + a_2)(r_1 + r_2) - b_1 - c - b_2, \tag{6}$$

and (6) can be written in the form

$$r_1^2 + r_1r_2 + r_2r_1 + r_2^2 = a_1r_1 + a_2r_1 \\ - a_1r_2 + a_2r_2 - b_1 - c - b_2,$$

which by (4) and (5) reduces to

$$r_1r_2 + r_2r_1 = a_2r_1 + a_1r_2 - c. \tag{7}$$

Let us now consider two elements $u_0+u_1r_1+u_2r_2$ and $u_0+u_1r_1'+u_2r_2'$. Their sum is $2u_0+u_1a_1+u_2a_2$ and their product is $Q(u_0, u_1, u_2)$ and hence the u_0, u_1, u_2 being numbers of K we see that the sum and product are numbers of K and hence the two elements as given are a pair of conjugate roots of a quadratic equation in K.

We shall now form a new extension of K by the adjunction of the two elements r_1 and r_2 subject to the above specified conditions and further assume that r_1r_2 and r_2r_1 are also roots of quadratic equations. We also suppose that

$$S(r_1r_2 + r_2r_1) = S(r_1r_2) + S(r_2r_1). \tag{8}$$

Let $q(x)=0$ be the quadratic equation of which r_1r_2 is a root. Using the associative law, which we shall also assume, we have

$$\frac{1}{r_1}(r_1r_2)r_1 = r_2r_1,$$

$$\frac{1}{r_1}(r_1r_2)^2r_1 = \frac{1}{r_1}(r_1r_2)r_1\frac{1}{r_1}(r_1r_2)r_1 = (r_2r_1)(r_2r_1) = (r_2r_1)^2\,;$$

and hence

$$\frac{1}{r_1}q(r_1r_2)r_1 = q(r_2r_1).$$

Since $q(r_1r_2)=0$, it follows that $q(r_2r_1)=0$ and r_1r_2 and r_2r_1 are roots of the same equation, and $S(r_1r_2)=S(r_2r_1)$. As above, we here assume that b_1 and b_2 are not zero. It would suffice to make this assumption regarding only one of them. Using (7), and (8), we then have

$$\begin{aligned} S(r_1r_2) + S(r_2r_1) &= 2S(r_1r_2) = a_2S(r_1) + a_1S(r_2) - 2c \\ &= 2a_1a_2 - 2c. \end{aligned}$$

Thus

$$S(r_1r_2) = a_1a_2 - c = a_{12}, \tag{9}$$

where for the present we use a_{12} to denote the trace of r_1r_2. The conjugate root $(r_1r_2)'$ of r_1r_2 is then $a_{12}-r_1r_2$.

If we now use the equations (3), we have

$$\begin{aligned} a_{12} &= a_1a_2 - r_1r_2' - r_2r_1' = a_1a_2 - r_1(a_2 - r_2) - (a_2 - r_2')r_1' \\ &= a_1a_2 - a_2(r_1 + r_1') + r_1r_2 + r_2'r_1' \\ &= a_1a_2 - a_1a_2 + r_1r_2 + r_2'r_1'. \end{aligned}$$

Therefore $r_2'r_1' = a_{12} - r_1r_2$, and we conclude that $r_2'r_1'$ is the conjugate of r_1r_2. We shall denote r_1r_2 by r_{12} and $r_2'r_1'$ by r_{12}'. We now have the following relations:

$$r_1r_{12} = r_1r_1r_2 = r_1^2r_2 = a_1r_1r_2 - b_1r_2 = a_1r_{12} - b_1r_2, \tag{10}$$

$$r_{12}r_2 = r_1r_2r_2 = r_1r_2^2 = a_2r_1r_2 - b_2r_1 = a_2r_{12} - b_2r_1, \tag{11}$$

$$\begin{aligned} r_{12}r_1 &= r_1(r_2r_1) = r_1(a_2r_1 + a_1r_2 - c - r_1r_2) \\ &= a_2(a_1r_1 - b_1) + a_1r_{12} - cr_1 - a_1r_{12} + b_1r_2 \\ &= -a_2b_1 + a_{12}r_1 + b_1r_2, \end{aligned} \tag{12}$$

$$\begin{aligned} r_2r_{12} &= (r_2r_1)r_2 = (a_2r_1 + a_1r_2 - c - r_1r_2)r_2 \\ &= a_2r_{12} + a_1a_2r_2 - a_1b_2 - cr_2 - a_2r_{12} + b_2r_1 \\ &= -a_1b_2 + b_2r_1 + a_{12}r_2. \end{aligned} \tag{13}$$

The equations (4), (5), (10), (11), (12), (13) can be summed up in the following multiplication table.

	1	r_1	r_2	r_{12}
1	1	r_1	r_2	r_{12}
r_1	r_1	$a_1r_1 - b_1$	r_{12}	$- b_1r_2 + a_1r_{12}$
r_2	r_2	$- c + a_2r_1 + a_1r_2 - r_{12}$	$a_2r_2 - b_2$	$- a_1b_2 + b_2r_1 + a_{12}r_2$
r_{12}	r_{12}	$- a_2b_1 + a_{12}r_1 + b_1r_2$	$- b_2r_1 + a_2r_{12}$	$a_{12}r_{12} - b_1b_2$

Let us now consider the extension of K consisting of all elements of the form $x_0+x_1r_1+x_2r_2+x_{12}r_{12}$, where x_0, x_1, x_2, and x_{12} are numbers of K. We have seen that r_1r_2 and $r_2'r_1'$ are a pair of conjugate roots of a quadratic equation. Let us next consider r_1r_{12} and $r_{12}'r_1'$. Their product is $b_1^2b_2$, a number of K. From the multiplication table

$$
\begin{aligned}
r_1r_{12} &= -b_1r_2 + a_1r_{12},\\
r_{12}'r_1' &= (a_{12} - r_{12})(a_1 - r_1) = a_1a_{12} - a_{12}r_1\\
&\qquad\qquad\qquad\qquad\qquad - a_1r_{12} + r_{12}r_1\\
&= a_1a_{12} - a_{12}r_1 - a_1r_{12} - a_2b_1 + a_{12}r_1 + b_1r_2\\
&= a_1a_{12} - a_2b_1 + b_1r_2 - a_1r_{12},
\end{aligned}
$$

whence

$$r_{12}'r_1' = - b_1r_2' + a_1r_{12}',$$

and

$$r_1r_{12} + r_{12}'r_1' = a_1a_{12} - a_2b_1,$$

a number of K. Hence as before r_1r_{12} and $r_{12}'r_1'$ are a pair of conjugate roots of a quadratic equation with coefficients in K, and $S(r_1r_{12}) = a_1a_{12} - a_2b_1$. In the same way we can show that $S(r_{12}r_1) = a_1a_{12} - a_2b_1$ and $S(r_2r_{12}) = S(r_{12}r_2) = a_2a_{12} - b_2a_1$ and in all cases the conjugate of the product is the product of the conjugates in reversed order. Hence

$$
\begin{aligned}
- a_2b_1 &= S(r_{12}r_1) - S(r_1)S(r_{12}),\\
- a_1b_2 &= S(r_{12}r_2) - S(r_2)S(r_{12}).
\end{aligned}
\tag{14}
$$

From the multiplication table

$$r_1 r_{12} + r_{12} r_1 = - a_2 b_1 + a_{12} r_1 + a_1 r_{12}, \tag{15}$$

$$r_2 r_{12} + r_{12} r_2 = - a_1 b_2 + a_{12} r_2 + a_2 r_{12}. \tag{16}$$

By (14) and the equation $-c = a_{12} - a_1 a_2$, we can then write a common form for (7), (15), (16) as follows:

$$r_i r_j + r_j r_i = S(r_i r_j) - S(r_i) S(r_j) + S(r_j) r_i + S(r_i) r_j. \tag{17}$$

From this we get

$$\begin{aligned} r_i r_j' + r_j r_i' &= r_i(a_j - r_j) + r_j(a_i - r_i) \\ &= S(r_j) r_i + S(r_i) r_j - r_i r_j - r_j r_i \\ &= S(r_i) S(r_j) - S(r_i r_j), \end{aligned} \tag{18}$$

which is a number of K. Let us now consider two elements

$$\begin{aligned} \xi &= x_0 + x_1 r_1 + x_2 r_2 + x_{12} r_{12}, \\ \xi' &= x_0 + x_1 r_1' + x_2 r_2' + x_{12} r_{12}'. \end{aligned}$$

Then $\xi + \xi' = 2x_0 + a_1 x_1 + a_2 x_2 + a_{12} x_{12}$ a member of K. Also

$$\begin{aligned} \xi\xi' = {} & x_0^2 + b_1 x_1^2 + b_2 x_2^2 + b_1 b_2 x_{12}^2 + a_1 x_0 x_1 + a_2 x_0 x_2 \\ & + a_{12} x_0 x_{12} + (r_1 r_2' + r_2 r_1') x_1 x_2 \\ & + (x_1 x_{12}' + r_{12} r_1') x_1 x_{12} + (r_2 r_{12}' + r_{12} r_2') x_2 x_{12}, \end{aligned} \tag{19}$$

and it may be shown that $\xi\xi' = \xi'\xi$. By (18) and (19) we see that $\xi\xi'$ is also a number of K and hence ξ and ξ' are a pair of conjugate roots of a quadratic equation with coefficients in K.

Consider next the two elements

$$\alpha = u_0 + u_1 r_1 + u_2 r_2 + u_{12} r_{12}, \quad \beta = v_0 + v_1 r_1 + v_2 r_2 + v_{12} r_{12}.$$

Then

$$\alpha \pm \beta = u_0 \pm v_0 + (u_1 \pm v_1) r_1 + (u_2 \pm v_2) r_2 + (u_{12} \pm v_{12}) r_{12}$$

and by the multiplication table we can also express the product in the same form. Hence the set of elements is closed with respect to addition, subtraction, and multiplication.

Since the product $r_i r_j$ is a linear function of r_1, r_2, r_{12} and its conjugate $r_j' r_i'$ is the same linear function of r_1', r_2', r_{12}' we see that $\alpha\beta$ and $\beta'\alpha'$ are the same linear function of r_1, r_2, r_{12} and r_1', r_2', r_{12}', respectively. Hence $\alpha\beta+\beta'\alpha'$ is a number of K and $\alpha\beta\cdot\beta'\alpha'=N(\alpha)N(\beta)$ is also a number of K. Therefore, in general for all products the conjugate of a product is the product of the conjugates in the reversed order.

If we let $r_0=r_0'=1$, we may write

$$\alpha\beta = \sum_{i,j} u_i v_j r_i r_j,$$

$$\beta\alpha = \sum_{i,j} u_i v_j r_j r_i,$$

whence we have

$$\begin{aligned}\alpha\beta+\beta\alpha &= \sum_{i,j} u_i v_j (r_i r_j + r_j r_i)\\ &= \sum_{i,j} u_i v_j [S(r_i r_j) - S(r_i)S(r_j) + S(r_i)r_j + S(r_j)r_i]\\ &= \sum_{i,j} u_i v_j S(r_i r_j) - \sum_i u_i S(r_i) \sum_j v_j S(r_j)\\ &\quad + \sum_i u_i S(r_i) \sum_j v_j r_j + \sum_j v_j S(r_j) \sum_i u_i r_i\\ &= S(\alpha\beta) - S(\alpha)S(\beta) + S(\alpha)\beta + S(\beta)\alpha.\end{aligned}$$

This shows that the equation (17) is true for any pair of elements α and β of the algebra.

5. *Extension of the Algebra.* Let us next consider a general quadratic form in $n+1$ variables

$$Q(x_0, x_1, x_2, \cdots, x_n) = \sum_{i,j} a_{ij} x_i x_j$$

having $a_{00}=1$ and $a_{ij}=a_{ji}$. From this we shall form n equations, each one being obtained by setting x for x_0 and one of the remaining variables equal to -1 and the rest equal to zero. The n equations are then

$$x^2 - a_{0i}x + a_{ii} = 0, \qquad (i = 1,2,3, \cdots, n).$$

The conjugate roots of these equations we shall denote by r_i and r_i' $(i=1, 2, \cdots, n)$. We shall also assume that r_i+r_j and $r_i'+r_j'$ are a pair of conjugate roots of the equation obtained from the equation

$$Q(x_0, x_1, x_2, \cdots, x_n) = 0$$

by putting $x_i = x_j = -1$, and all the remaining x_k, except x_0, equal to zero. We shall further assume that for any pair r_i, r_j all the conditions of the preceding sections are fulfilled so that $1, r_i, r_j, r_i r_j$ constitute the basal elements of an algebra such as we have already discussed. The product $r_i r_j$ we shall denote by r_{ij}.

All polynomials in $r_1, r_2, \cdots, r_n$ having coefficients in K constitute an algebra over K. In a later paper I expect to show some consequences of further restrictions on products involving three or more of the elements $r_1, r_2, \cdots, r_n$. For the present the algebra as defined is sufficient.

6. *A Linear Set.** Having thus defined the algebra let us consider all elements of the form $x_0 + x_1 r_1 + x_2 r_2 + \cdots + x_n r_n$. We shall write

$$\alpha = u_0 + u_1 r_1 + \cdots + u_n r_n,$$
$$\alpha' = u_0 + u_1 r_1' + \cdots + u_n r_n' .$$

Then

$$S(\alpha) = \alpha + \alpha' = 2u_0 + a_{01}u_1 + a_{02}u_2 + \cdots + a_{0n}u_n,$$
$$N(\alpha) = \alpha\alpha' = u_0^2 + \sum_{i=1}^{n} a_{ii}u_i^2 + \sum_{i=1}^{n} a_{0i}u_0u_i + \sum_{i<j} (r_i r_j' + r_j r_i')u_i u_j .$$

But according to our assumptions regarding the $r_1, r_2, \cdots, r_n$, by equations (18) and (9), we have

$$r_i r_j' + r_j r_i' = S(r_i)S(r_j) - S(r_i r_j) = a_{ij}.$$

We note that a_{ij} has a different meaning here from what it had in the preceding section where $a_{12} = S(r_1 r_2)$. Here a_{ij} has taken the place of the c.

Hence we see that $S(\alpha)$ and $N(\alpha)$ are both numbers of K, and any element α of the linear set is a root of a quadratic equation with coefficients in K. We also note that

$$N(\alpha) = Q(u_0, u_1, u_2, \cdots, u_n).$$

It is not difficult to show that $\alpha\,\alpha' = \alpha'\,\alpha$.

---

* Dickson, loc. cit.

If α is some particular element of the linear set, the set also contains $m\alpha+n$ and hence with $u_0+u_1r_1+\cdots+u_nr_n$ is also found in the set $u_1r_1+\cdots+u_nr_n$ and all its elements are obtained by the addition of a number of K to an element of the last form. But $u_1r_1+u_2r_2+\cdots+u_nr_n$ is a root of

$$Q(x, -u_1, -u_2, \cdots, -u_n) = 0.$$

We therefore see that we may consider the linear set as the totality of all quadratic extensions to K formed by the adjunction of the roots of all equations obtained from the equation $Q(x, x_1, x_2, \cdots, x_n) = 0$ by assigning to the $x_1, x_2, \cdots, x_n$ all possible combinations of values from K.

7. *Application to a Diophantine Equation.* We shall next consider the equation

$$(20) \qquad \sum_{i,j=0}^{n} a_{ij}x_ix_j = v_1v_2\cdots v_k, \qquad (a_{ij} = a_{ji}),$$

in which the coefficients a_{ii} and $2a_{ij}$ are rational integers. The application of the foregoing algebra will give a method for finding all rational, integral solutions of the equation. The unknowns are the $x_0, x_1, \cdots, x_n, v_1, v_2, \cdots, v_k$. The field K used in the preceding pages is, from now on, the field of rational numbers. If we multiply both members of (20) by a_{00} and put $a_{00}x_0=y_0$ we can write the left hand member of the equation as a quadratic form in $y_0, x_1, x_2, \cdots, x_n$. This form we shall denote by $Q(y_0, x_1, x_2, \cdots, x_n)$, and the equation (20) is equivalent to

$$(21) \qquad Q(y_0, x_1, x_2, \cdots, x_n) = a_{00}v_1v_2\cdots v_k.$$

The quadratic form $Q(y_0, x_1, \cdots, x_n)$ has rational integral coefficients with that of y_0^2 equal to 1 and hence is of the form considered in the preceding sections. The left hand member of (21) is therefore the norm of the general element of a linear set in an algebra such as has been defined above. It is therefore possible to write the equation (20) in a new form

$$(22) \quad N(a_{00}x_0 + r_1x_1 + r_2x_2 + \cdots + r_nx_n) = a_{00}v_1v_2\cdots v_k.$$

For each set of rational values of $x_1, x_2, \cdots, x_n$ a root $\theta(x)$ of the equation

$$(23) \qquad Q(x, x_1, x_2, \cdots, x_n) = 0$$

is a generator of a quadratic extension of K. This may be either of the first or second kind.

Let us consider first the case when (23) is irreducible so that the quadratic extension is of the first kind. Then θ generates a quadratic number field and 1, θ is a base of a ring in this field and (a_{00}, θ) is the base of an ideal in the ring. The problem of obtaining the solutions of

$$(24) \qquad N(a_{00}x_0 + \theta t) = a_{00}v_1v_2 \cdots v_k$$

has been solved by the author,* and from this we see that for those rational integral values of $x_1, x_2, \cdots, x_n$ which cause (23) to be irreducible we can obtain the solutions of (22) by writing it in the form

$$(25) \quad N(a_{00}x_0 + r_1x_1t + r_2x_2t + \cdots + r_nx_nt) = a_{00}v_1v_2 \cdots v_k$$

and assigning values to $x_1, x_2, \cdots, x_n$ and solving for x_0 and t by the method for solving (24).

In the case when the values $x_1, x_2, \cdots, x_n$ cause (23) to be reducible the left-hand member of (25) is the product of two linear factors which are homogeneous in x_0 and t. Then elementary methods suffice for the determination of x_0 and t, and the v_i.

It is easily seen that in assigning the values to $x_1, x_2, \cdots, x_n$ only such as are relatively prime need be used as all others will be included among the ones so found.

Hence to obtain all solutions of (20) replace $x_1, x_2, \cdots, x_n$ by $x_1t, x_2t, \cdots, x_nt$; assign to $x_1, x_2, \cdots, x_n$ arbitrary rational integral values thus reducing the left hand member of (20) to a binary form and hence solve by means of known methods.

UNIVERSITY OF MISSOURI

---

* This Bulletin, vol. 31, p. 430.