ON THE COMPOSITION OF QUADRATIC FORMS*

BY E. D. JENKINS

1. *Introduction.* A compound of two binary quadratic forms $f_1(x_1, y_1)$ and $f_2(x_2, y_2)$ is a third form $f(x, y)$ such that $f(x, y) = f_1(x_1, y_1)f_2(x_2, y_2)$ under a primitive bilinear transformation

$$x = p_1x_1x_2 + p_2x_1y_2 + p_3y_1x_2 + p_4y_1y_2,$$
$$y = q_1x_1x_2 + q_2x_1y_2 + q_3y_1x_2 + q_4y_1y_2.$$

The fundamental problem of this theory is to determine a compound of two given forms and the transformation under which the relationship exists.

This problem has been considered† by Gauss, Arndt, Dedekind and others. The method of Dedekind‡ was based upon a correspondence between forms and moduls in an algebraic field, composition of forms corresponding to multiplication of moduls.

The method of the present paper is also based upon a correspondence between forms and moduls. These moduls form a subclass of those considered by Dedekind in that only integral moduls are employed. These moduls in turn are in correspondence with matrices with rational integral elements, the greatest common divisor process corresponding to multiplication of moduls and hence to composition of forms. By this correspondence and the matric g. c. d. process of Châtelet,§ the composition of quadratic forms requires but a small fraction of the time and labor required by previously known methods.

2. *The Correspondence.* Let 1, θ be an integral basis for the quadratic field $\mathfrak{F}(\sqrt{m})$. Then $\theta^2 = m$ if $m \equiv 2, 3 \pmod 4$, (Case 1); and $\theta^2 = \theta + m', 4m' = m - 1$ if $m \equiv 1 \pmod 4$, (Case 2). Let a, b, and k be rational integers, of which a and k are positive, such that $b^2 - k^2 \equiv 0 \pmod a$, (Case 1); $b^2 + bk - k^2m' \equiv 0 \pmod a$, (Case 2).

* Presented to the Society, April 19, 1935.

† Gauss, *Disquisitiones Arithmeticae*, 1801, §234 ff.; Arndt, *Auflösung einer Aufgabe in der Composition der quadratischen Formen*, Journal für Mathematik, vol. 56 (1859), pp. 64–71.

‡ Dirichlet, *Vorlesungen über Zahlentheorie*, 4th ed., 1894, pp. 640–657.

§ A. Châtelet, *Groupes Abéliens Finis*, 1924, p. 26.

The general number $\alpha=\alpha_1x+\alpha_2y$ of the modul with basis

$$(1)\qquad \alpha_1 = a, \qquad \alpha_2 = b + k\theta$$

has the norm

$$N(\alpha) = a\left(ax^2 + 2bxy + \frac{b^2 - k^2m}{a}\, y^2\right),$$

$$N(\alpha) = a\left(ax^2 + (2b + k)xy + \frac{b^2 + bk - k^2m'}{a}\, y^2\right),$$

in Cases 1 and 2, respectively. We shall say that the form

$$(2)\qquad \begin{aligned} f(x, y) &= ax^2 + 2bxy + \frac{b^2 - k^2m}{a}\, y^2, \\ f(x, y) &= ax^2 + (2b + k)xy + \frac{b^2 + bk - k^2m'}{a}\, y^2, \end{aligned}$$

is associated with the basis (1) and also with the matrix

$$(3)\qquad G = \begin{pmatrix} a & 0 \\ b & k \end{pmatrix}.$$

The fact that we consider only irreducible forms makes it necessary that $a\neq 0$ and $k\neq 0$.

The totality of bases of the above modul is given by

$$(4)\qquad \beta_1 = c_{11}\alpha_1 + c_{12}\alpha_2, \qquad \beta_2 = c_{21}\alpha_1 + c_{22}\alpha_2,$$

where α_1, α_2 is the basis (1) and the c_{ij} are rational integers of determinant ± 1. Then all bases of the modul have matrices of the form CG, where $C=(c_{ij})$ is a unimodular matrix with rational integral elements.

Let $\beta=\beta_1x_1+\beta_2y_1$. Define the transformation

$$(5)\qquad X = c_{11}x_1 + c_{21}y_1, \qquad Y = c_{12}x_1 + c_{22}y_2$$

of determinant ± 1. Then $\beta\ \ \alpha_1X+\alpha_2Y$, and in Cases 1 and 2, respectively,

$$f_1(x_1, y_1) = \frac{N(\beta)}{a} = aX^2 + 2bXY + \frac{b^2 - k^2m}{a}\, Y^2,$$

$$= aX^2 + (2b + k)XY + \frac{b^2 + bk - k^2m'}{a}\, Y^2,$$

is a quadratic form which, by (5), is either properly or improperly equivalent to $f(x, y)$. Since every basis of the modul can be reduced by a transformation of determinant $+1$ either to the basis $(a, b+k\theta)$ or to the basis $(-a, b+k\theta)$, the form represented by any basis of the modul is properly equivalent either to the form (2) or to its opposite,

$$\begin{aligned} g(x, y) &= ax^2 - 2bxy + \frac{b^2 - k^2m}{a} y^2, \\ &= ax^2 - (2b + k)xy + \frac{b^2 + bk - k^2m'}{a} y^2, \end{aligned}$$

in Cases 1 and 2, respectively. However, the form $g(x, y)$ can be represented by the matrix

$$G' = \begin{pmatrix} a & 0 \\ -b & k \end{pmatrix}, \text{(Case 1)}, \qquad G' = \begin{pmatrix} a & 0 \\ -(b+k) & k \end{pmatrix}, \text{(Case 2)},$$

with a and k positive, so we need employ only matrices of type (3), or matrices which can be reduced to type (3) by a transformation of determinant $+1$.

Next, consider an irreducible form

$$(6) \qquad f(x, y) = ax^2 + Bxy + cy^2, \qquad (a > 0).$$

The problem is to determine what integral algebraic modul will define the above form.

Consider the discriminant $d = B^2 - 4ac = l^2m$, where m contains no square factor greater than 1. Consequently $m \equiv 1, 2,$ or 3 (mod 4). If $m \equiv 1$ (mod 4), $B^2 \equiv l^2$ (mod 4) implies $B - l$ is even. Hence we define integers b and k such that $k = l$, $2b + k = B$. If $m \equiv 2$, 3 (mod 4), $B^2 \equiv l^2m$ (mod 4) can hold only if B and l are both even. Hence we define $2k = l$, $2b = B$. In either case

$$\alpha_1 = a, \qquad \alpha_2 = b + k\theta$$

is a modul of type (1), whose existence we supposed, and this modul yields form (6).

We wish to determine a necessary and sufficient condition that a matrix of positive determinant and having k as the positive g. c. d. of the elements of the second column, correspond to a quadratic form.

Let Γ be the matrix*

* C. C. MacDuffee, Annals of Mathematics, (2), vol. 29 (1928), p. 200.

$$\Gamma = \begin{pmatrix} 0 & 1 \\ m & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ m' & 1 \end{pmatrix}$$

for Cases 1 and 2. Consider first a matrix of type (3). In Case 1, let

$$\begin{pmatrix} a & 0 \\ b & k \end{pmatrix}\begin{pmatrix} 0 & k \\ km & 0 \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} a & 0 \\ b & k \end{pmatrix}.$$

Then

$$\begin{aligned} 0 &= ea + fb, & ak &= fk, \\ k^2m &= ga + hb, & bk &= hk. \end{aligned}$$

Since $k \neq 0$, we see that $f = a$, $h = b$, $e = -b$, $g = -(b^2 - k^2m)/a$ are rational integers if G corresponds to a form. Conversely if

$$\begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

is a matrix with rational integral elements, $b^2 - k^2m \equiv 0 \pmod{a}$ and G is a matrix of a form. The proof for Case 2 is similar.

If G' is any non-singular matrix of positive determinant, then* $G' = CG$, where C is an integral matrix of determinant $+1$, and G is a matrix of type (3). If G' is a matrix of a form, then $G = G^{\mathrm{I}}G'$ is also a matrix of a form, whence, by the above proof,

$$G k \Gamma = \Lambda' G, \tag{7}$$

where Λ' is a matrix with rational integral elements. Hence

$$G' k \Gamma = C \Lambda' C^{\mathrm{I}} G' \tag{8}$$

where $C\Lambda C^{\mathrm{I}}$ is also a matrix with integral elements. Since (8) also implies (7), we have proved the following theorem.

THEOREM 1. *A necessary and sufficient condition that a non-singular matrix G', of positive determinant, the g. c. d. of the elements of whose second column is k, represent a quadratic form of discriminant $4k^2m$ (Case 1), k^2m (Case 2), is that*

$$G' k \Gamma = \Lambda G',$$

where Λ is a matrix with rational integral elements.

* C. C. MacDuffee, *Theory of Matrices*, 1933, p. 32.

3. *Product of Moduls.* We define the second or S-matrix of any algebraic number $\beta = b_1 + b_2\theta$ to be the matrix

$$S(\beta) = b_1\mathrm{I} + b_2\Gamma,$$

where I is the identity matrix and Γ is defined as above. The theorem which was proved* for ideal multiplication in a linear algebra holds for the multiplication of integral algebraic moduls. That is, if G_1 and G_2 are the basis matrices of the moduls $M_1 = [\alpha_1, \alpha_2]$ and $M_2 = [\beta_1, \beta_2]$, a matrix of the product modul M is a greatest common right divisor of $G_1S(\beta_1)$ and $G_1S(\beta_2)$. We shall prove the following theorem.

THEOREM 2. *A matric g. c. r. d. (of positive determinant) of $G_1S(\beta_1)$ and $G_1S(\beta_2)$ represents a quadratic form.*

Let the two given matrices, representing forms $f_1(x_1, y_1)$ and $f_2(x_2, y_2)$ be

$$G_1 = \begin{pmatrix} a_1 & 0 \\ b_1 & k_1 \end{pmatrix}, \quad G_2 = \begin{pmatrix} a_2 & 0 \\ b_2 & k_2 \end{pmatrix}.$$

The matric g. c. r. d. of $G_1S(\beta_1)$ and $G_1S(\beta_2)$ may be put into the form

$$G = \begin{pmatrix} a & 0 \\ b & k \end{pmatrix},$$

where a and k are positive integers. Moreover†

$$\begin{pmatrix} G_1S(\beta_1) & 0 \\ G_1S(\beta_2) & 0 \end{pmatrix} \overset{\mathrm{L}}{=} \begin{pmatrix} G & 0 \\ 0 & 0 \end{pmatrix}. \tag{9}$$

Case 1.

$$G_1S(\beta_1) = \begin{pmatrix} a_1a_2 & 0 \\ b_1a_2 & k_1a_2 \end{pmatrix}, \quad G_1S(\beta_2) = \begin{pmatrix} a_1b_2 & a_1k_2 \\ b_1b_2 + k_1k_2m & b_1k_2 + k_1b_2 \end{pmatrix}.$$

By (9), comparing elements in the first row and second column on both sides of the matric equation, we see that $0 = q_1k$. Since $k \neq 0$, $q_1 = 0$, and by comparing elements in the first row and first column, we see that there exists an integer p_1 such that

* Grace Shover and C. C. MacDuffee, this Bulletin, vol. 37 (1931), pp. 434–38.

† A. Châtelet, *Groupes Abéliens Finis*, 1924, p. 26.

$$(10) \qquad a_1a_2 = p_1a.$$

Also from (9) it is seen that there exist rational integers p, q, r, s such that

$$\begin{aligned} b &= pa_1a_2 + qb_1a_2 + ra_1b_2 + s(b_1b_2 + k_1k_2m), \\ k &= qk_1a_2 + ra_1k_2 + s(b_1k_2 + k_1b_2). \\ b^2 - k^2m &\equiv q^2a_2^2(b_1^2 - k_1^2m) + r^2a_1^2(b_2^2 - k_2^2m) \\ &\quad + s^2(b_1^2 - k_1^2m)(b_2^2 - k_2^2m) \\ &\quad + 2qsa_2b_2(b_1^2 - k_1^2m) + 2rsa_1b_1(b_2^2 - k_2^2m) \\ &\equiv q^2a_2^2a_1c_1 + r^2a_1^2a_2c_2 + s^2a_1a_2c_1c_2 + 2qsb_2c_1a_1a_2 \\ &\quad + 2rsb_1c_2a_1a_2 \\ &\equiv 0 \pmod{a_1a_2} \equiv 0 \pmod{a}. \end{aligned}$$

Similarly, in Case 2, $b^2+bk-k^2m' \equiv 0 \pmod{a}$.

Since the g. c. r. d., taken in the form above, represents a quadratic form, any g. c. r. d. of positive determinant will also represent a form.

Let the general numbers of the moduls represented by matrices G_1, G_2, and G be

$$\alpha = a_1x_1 + (b_1 + k_1\theta)y_1, \qquad \beta = a_2x_2 + (b_2 + k_2\theta)y_2,$$
$$\gamma = ax + (b + k\theta)y.$$

There exists a primitive bilinear transformation under which $\alpha\beta = \gamma$. Then, since $N(\alpha)N(\beta) = N(\gamma)$, it follows that

$$a_1a_2f_1(x_1, y_1)f_2(x_2, y_2) = a\phi(x, y),$$

where ϕ is the form represented by matrix G. By (10), we have the following theorem.

THEOREM 3. *The form $\phi(x, y)$, represented by a matric g. c. r. d. of $G_1S(\beta_1)$ and $G_1S(\beta_2)$, is such that*

$$p_1f_1(x_1, y_1)f_2(x_2, y_2) = \phi(x, y),$$

where p_1 is the integer defined by (10).

Dedekind has established* a correspondence between binary

* Dirichlet, *Zahlentheorie*, 4th ed., §187.

quadratic forms and algebraic moduls. The moduls we consider form a subset of those considered by Dedekind, but a subset which is very convenient from the computational standpoint.

Let the matrix G, given by (3), correspond to the form $f(x, y)$. By the Dedekind theory, the algebraic number $\omega = (b/a) + (k/a)\theta$ satisfies the irreducible equation

$$\frac{1}{l}\left(a\omega^2 - 2b\omega + \frac{b^2 - k^2m}{a}\right) = 0, \qquad \text{(Case 1)},$$

$$\frac{1}{l}\left(a\omega^2 - (2b + k)\omega + \frac{b^2 + bk - k^2m'}{a}\right) = 0, \qquad \text{(Case 2)},$$

where l is the g. c. d. of a, $2b$, $(b^2 - k^2m)/a$, or of a, $2b+k$, $(b^2+bk-k^2m')/a$ for the respective cases. If $f'(x, y)$ denotes the form corresponding to the matrix G under the Dedekind theory, $f(x, y) = lf'(x, y)$, where l is the g. c. d. of the coefficients of $f(x, y)$. It is also clear* that for the modul M, corresponding to G, the norm $N(M) = a^2 \div (a/l) = al$. Since

$$N(M_1)N(M_2) = N(M),$$

where modul M is the product of moduls M_1 and M_2, it follows that $a_1a_2l_1l_2 = al$. Since, by (10), $a_1a_2 = p_1a$, the above equation becomes

$$(11) \qquad p_1l_1l_2 = l \quad \text{or} \quad l_1l_2 = l/p_1.$$

If f_1', f_2', and f' are the forms corresponding to moduls M_1, M_2, and M under the Dedekind theory, then $f_1'f_2' = f'$, where f' is a compound of f_1' and f_2'. Multiplying both sides of this equation by (11_2), we have $f_1(x_1, y_1)f_2(x_2, y_2) = f(x, y)$, where f is a compound of f_1 and f_2. But f_1 and f_2 correspond to matrices G_1 and G_2, while the form $\phi(x, y) = lf' = p_1f(x, y)$ corresponds to G. Hence we have the following theorem.

THEOREM 4. *The form $\phi(x, y)$ which corresponds to a g. c. r. d. of $G_1S(\beta_1)$ and $G_1S(\beta_2)$ is such that $\phi(x, y) = p_1f(x, y)$, where $f(x, y)$ is a compound of $f_1(x_1, y_1)$ and $f_2(x_2, y_2)$, and $p_1 = a_1a_2/a$ is an integer.*

4. *Conclusion.* A computational method for the composition of forms is now at our disposal. Furthermore, if we restrict our

* Ibid.

matrices to reduced forms, the element in the upper right corner being a 0, the form may be read directly from the matrix without reference to the modul it defines. For other forms of the matrix we can find the corresponding binary form from the norm of the general number defined by the matrix. In either case we have a simple and direct method for determining a compound of two given forms.

As an example, let us take $f_1(x_1, y_1) = 5x_1^2 + 2x_1y_1 + 5y_1^2$, and $f_2(x_2, y_2) = 77x_2^2 + 20x_2y_2 + 2y_2^2$. Their discriminants are $d_1 = -96 = 16(-6)$ and $d_2 = -216 = 36(-6)$, so the forms are associated with the field $\mathfrak{F}(\sqrt{-6})$. Since $-6 \equiv 2 \pmod 4$,

$$\Gamma = \begin{pmatrix} 0 & 1 \\ -6 & 0 \end{pmatrix}.$$

We note that $16(-6) = 4k_1^2m = -24k_1^2$ and $36(-6) = -24k_2^2$, whence $k_1 = 2$, $k_2 = 3$. Then

$$G_1 = \begin{pmatrix} 5 & 0 \\ 1 & 2 \end{pmatrix}, \qquad G_2 = \begin{pmatrix} 77 & 0 \\ 10 & 3 \end{pmatrix}.$$

$$G_1S(\beta_1) = \begin{pmatrix} 385 & 0 \\ 77 & 154 \end{pmatrix}, \qquad G_1S(\beta_2) = \begin{pmatrix} 50 & 15 \\ -26 & 23 \end{pmatrix}.$$

$$\begin{Bmatrix} 385 & 0 & 0 & 0 \\ 77 & 154 & 0 & 0 \\ 50 & 15 & 0 & 0 \\ -26 & 23 & 0 & 0 \end{Bmatrix} \overset{L}{=} \begin{Bmatrix} 385 & 0 & 0 & 0 \\ 183 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{Bmatrix},$$

so

$$G = \begin{pmatrix} 385 & 0 \\ 183 & 1 \end{pmatrix},$$

and, since $p_1 = 1$, the compound is the form

$$f = 385x^2 + 366xy + 87y^2.$$

By equating the coefficients of 1 and θ in the equation $\alpha\beta = \gamma$, the bilinear transformation is found to be

$$\begin{aligned} x &= x_1x_2 - 7x_1y_2 - 73x_2y_1 - 11y_1y_2, \\ y &= \phantom{x_1x_2 - {}} 15x_1y_2 + 154x_2y_1 + 23y_1y_2. \end{aligned}$$

THE OHIO STATE UNIVERSITY