# COMPOSITION OF BINARY QUADRATIC FORMS

GORDON PALL

1. **Introduction.** The composition of quadratic forms, as originated by Gauss,[1] is based on bilinear transformations. Thus, if a quadratic form $f_1 = \sum a_{ij}x_ix_j$ is expressible as a product of two forms $f_2(y_1, \cdots, y_n)$ and $f_3(z_1, \cdots, z_n)$ by means of a bilinear substitution $x_\alpha = \sum a_{\alpha\beta\gamma}y_\beta z_\gamma$, and if the determinants of order $n$ in the $n$-by-$n^2$ matrix $(a_{\alpha\beta\gamma})$ are relative prime, $f_1$ is called the compound, or product under composition, of $f_2$ and $f_3$. There are few examples of composition except for quadratic forms, and there it is confined to certain classes of forms in two, four, and eight variables.

Now there is evidence that quadratic forms not admitting composition have certain properties akin to those which are most easily established in the case of binaries by use of composition. This suggests that the use of bilinear transformations is too restrictive, and that other useful definitions of composition may be possible. Dirichlet[2] did in fact base a theory of composition of binary quadratic forms on the representation of numbers. However, bilinear transformations appear (loc. cit., p. 159, formula (5)) in his proof of the uniqueness of the product class. Again, Brandt[3] gave a theory of composition for binaries, based on integral linear transformations of a Grundform into multiples of the binary quadratic forms of a given discriminant. The extension of this to $n$ variables appears to be difficult.

In this article we define a compound of binary quadratic forms in a manner basically related to that of Dirichlet; and prove the uniqueness of the product class without using bilinear transformations. We also show that the basic lemma (due to Gauss) can be extended to quadratic forms in $n$ variables. All the usual consequences of composition of binary quadratic forms can be derived from our present approach, some of them more simply. But we shall not enter into these details here.

2. **Gauss's lemma and its generalization.** The basic lemma of

Presented to the Society, December 31, 1947; received by the editors January 12, 1948.

[1] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801, Articles 235–249 et. seq.

[2] G. L. Dirichlet, *De formarum binarum secundi gradus compositione*, Berlin, 1851. Reprinted in Journal für Mathematik vol. 47 (1854) pp. 155–160; Werke, II, 1897, pp. 105–114. French translation, Journal de Mathematik (2) vol. 4 (1859) pp. 389–398. Also, Dirichlet-Dedekind, *Zahlentheorie*, Supplement X, §§145–9, 1871, 1879, 1894.

[3] H. Brandt, Journal für Mathematik vol. 150 (1919) pp. 1–46.

Gauss gives a criterion for equivalence of binary quadratic forms. Let $[a, b, c]$ denote the real form $ax^2+bxy+cy^2$. If $[a, b, c]$ is carried into $[a', b', c']$ by the unimodular transformation

$$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y', \qquad \alpha\delta - \beta\gamma = 1, \tag{1}$$

then $c' = a\beta^2 + b\beta\delta + c\delta^2$, and

$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2, \qquad b' = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta. \tag{2}$$

From (2) it is easily seen that

$$\begin{gathered} \{a\alpha + 2^{-1}(b + b')\gamma\}/a' \quad \textit{and} \\ \{2^{-1}(b - b')\alpha + c\gamma\}/a' \quad \textit{are integral}; \end{gathered} \tag{3}$$

indeed these expressions are equal, respectively, to $\delta$ and $-\beta$. Gauss's lemma is as follows:

LEMMA 1. *The real forms* $[a, b, c]$ *and* $[a', b', c']$ *with* $a' \neq 0$ *are equivalent if and only if their discriminants are equal and there exist two integers* $\alpha$ *and* $\gamma$ *satisfying* $(2_1)$ *and* (3).

Indeed, if the expressions in (3) are denoted by $\delta$ and $-\beta$, then $\alpha\delta + \gamma(-\beta) = (a\alpha^2 + b\alpha\gamma + c\gamma^2)/a' = 1$, and $0 = a'(\beta\delta + \delta(-\beta)) = a\alpha\beta + 2^{-1}b(\alpha\delta + \beta\gamma) + c\gamma\delta - 2^{-1}b'$, in agreement with (2). Hence the transformation (1) replaces $[a, b, c]$ by $[a', b', c'']$, where $b'^2 - 4a'c'' = b'^2 - 4a'c'$, $c'' = c'$.

To extend this criterion to $n$-ary quadratic forms, consider a symmetric, nonsingular matrix $A$ of order $n$. Apply to $A$ the unimodular transformation of matrix $T = (T_1\, T_2)$, where $T_1$ has $n-1$ columns, and $T_2$ one column, and obtain

$$B = T'AT = \begin{bmatrix} B_1 & K' \\ K & B_2 \end{bmatrix}, \tag{4}$$
$$\text{where} \quad B_1 = T_1'AT_1, \; K = T_2'AT_1, \; B_2 = T_2'AT_2.$$

Thus, if $A$ and $B$ are equivalent matrices, then the leading minor matrix $B_1$ of order $n-1$ of $B$ is represented primitively by $A$, the representation being $T_1$. Also, if $S' = T^{-1}$, $S = (S_1\, S_2)$ can be partitioned similarly to $T$, with $S_2$ a single column. It should be noted that $S_2$ is uniquely determined by $T_1$ alone, since $S_2$ is the column of cofactors in $T$ of its last column. Also,

$$T_1'S_1 = I_1, \quad T_1'S_2 = 0, \quad T_2'S_1 = 0, \quad T_2'S_2 = 1,$$

where $I_1$ is the identity matrix of order $n-1$. Finally, notice that

$$T'AT_1 = \begin{bmatrix} B_1 \\ K \end{bmatrix}, \quad \text{hence} \quad AT_1 = S_1B_1 + S_2K.$$

Thus $(AT_1 - S_2K)B_1^{-1}$ is an integral matrix. This is the analogue of condition (3) above. We are now ready to state and prove the generalization of Lemma 1:

THEOREM 1. *Let $A$ and $B$ denote symmetric nonsingular matrices of order $n$, of equal determinants. Partition $B$ as follows, with $B_1$ of order $n-1$ and $B_2$ a number*:

$$B = \begin{bmatrix} B_1 & K' \\ K & B_2 \end{bmatrix}. \tag{5}$$

*Let $T_1$ (with $n$ rows, $n-1$ columns) be an integral matrix such that $B_1 = T_1'AT_1$. Denote by $S_2$ the column vector of cofactors consisting of the minor determinants of order $n-1$ of $T_1$ taken with appropriate signs. Assume that $(AT_1 - S_2K)B_1^{-1}$ is an integral matrix. Then $A$ and $B$ are equivalent, and it is possible to construct $T_2$ so that $(T_1\ T_2)$ is a unimodular transformation of $A$ into $B$.*

PROOF. Set $(AT_1 - S_2K)B_1^{-1} = S_1$. It is not clear whether $(S_1\ S_2)$ is then unimodular. However, the equation $AT_1 = S_1B_1 + S_2K$ yields $T_1'AT_1 = T_1'S_1B_1 + T_1'S_2K$, $B_1 = T_1'S_1B_1$, and since $B_1$ is assumed to be nonsingular, $T_1'S_1 = I_1$. This implies that $T_1$ is primitive, that is, the minor determinants of order $n-1$ of $T_1$ are relatively prime. Hence, the most general integral matrix $R_1$ (with $n$ rows and $n-1$ columns) satisfying $T_1'R_1 = I_1$ is given by $R_1 = S_1 + S_2H$, where $H$ is an arbitrary integral matrix of one row and $n-1$ columns. Indeed, if $R_1 - S_1 = X$, then each column $x_i$ of $X$ is a solution of $T_1'x_i = 0$; since $T_1$ is primitive, this solution is $x_i = S_2h_i$ where $h_i$ is an integer. Since $T_1$ is primitive, there exists a column $T_2$ such that $(T_1\ T_2)$ is unimodular, and $(T_1\ T_2)^{-1} = (R_1\ S_2)'$, where $R_1$ is thus a solution of $T_1'R_1 = I_1$. Hence $R_1 = S_1 + S_2H$, for some integral $H$, and $(S_1\ S_2)' = (T_1\ T_1H' + T_2)$. Accordingly, we can rename $T_1H' + T_2$ as $T_2$, and have $(S_1\ S_2)' = (T_1\ T_2)^{-1}$. Then $T_2'AT_1 = T_2'(S_2K + S_1B_1) = K$. The value of $B_2$ is fixed by the equality of the determinants of $A$ and $B$. The theorem follows.

This theorem opens the way to a possible extension of the methods of this article to $n$ variables.

3. **Preliminary lemmas.** As a first application of Lemma 1, we have the following lemma.

LEMMA 2. *Let $a$, $a_1$, $a_2$, $b$, $c$ be integers, $aa_2 \neq 0$. Then $[a_1, b, aa_2c] \sim [a_2, b, aa_1c]$ implies that $[aa_1, b, a_2c] \sim [aa_2, b, a_1c]$. If $(a, b, c) = 1$,* *then the equivalence of the latter two forms implies that of the former.*

PROOF. By Lemma 1, the equivalence of the first two forms is tantamount to the existence of integers $\alpha$ and $\nu$ satisfying

$$(6)\qquad a_2 = a_1\alpha^2 + b\alpha\nu + aa_2c\nu^2,\ a_1\alpha + b\nu \equiv 0,\ aa_2c \equiv 0 \pmod{a_2};$$

and the equivalence of the last two forms amounts to

$$(7)\quad aa_2 = aa_1\alpha^2 + b\alpha\gamma + a_2c\gamma^2,\ aa_1\alpha + b\gamma \equiv 0,\ a_2c\gamma \equiv 0 \pmod{aa_2},$$

with some integers $\alpha, \gamma$. If (6) holds, defining $\gamma = a\nu$ yields (7). If (7) holds, then $a|b\gamma$ and $a|c\gamma$, and hence if $(a, b, c) = 1$, $a|\gamma$, and $\nu = \gamma/a$ is an integer.

The importance of this lemma may be seen from

LEMMA 3. *For any primitive binary quadratic forms $\phi_1, \cdots, \phi_q$ of the same discriminant $d$, there can be found integers $b, s, a_1, \cdots, a_q$ such that*

$$(8)\qquad \phi_i \sim [a_i, b, sa_1 \cdots a_q/a_i] \qquad (i = 1, \cdots, q).$$

*Furthermore, these integers can be chosen so that $a_1, \cdots, a_q$, and $2d$ are coprime in pairs.*

PROOF. A primitive form represents primitively integers prime to any assigned integer, and any integer primitively represented can be taken to be the first coefficient of an equivalent form. Choose for $a_1$ any integer primitively represented by $\phi_1$ and prime to $2d$; for $a_2$ any integer primitively represented by $\phi_2$ and prime to $2a_1d$; $\cdots$; and, finally, for $a_q$ any integer primitively represented by $\phi_q$ and prime to $2a_1 \cdots a_{q-1}d$. Then the $\phi_i$ are equivalent to respective forms $[a_i, b_i, c_i]$ $(i=1, \cdots, q)$. By the Chinese Remainder Theorem, an integer $b$ can be chosen to satisfy

$$(9)\qquad b \equiv b_i \pmod{2a_i} \qquad (i = 1, \cdots, q).$$

Then $\phi_i \sim [a_i, b, h_i]$, where $d = b^2 - 4a_ih_i$ $(i=1, \cdots, q)$, and hence since $a_1, \cdots, a_q$, 2 are coprime in pairs, $d = b^2 - 4a_1 \cdots a_qr$, with $r$ an integer.

**4. Composition of binary quadratic forms.** By the preceding lemma, there can be constructed within any two primitive classes $C_1$ and $C_2$, not necessarily distinct, of binary quadratic forms of the same discriminant, *united* forms of the type

$$(10)\qquad \phi_1 = [a_1, b_1, a_2c_1] \text{ in } C_1, \qquad \phi_2 = [a_2, b_1, a_1c_1] \text{ in } C_2.$$

This is easily seen to be true when the classes are not primitive, if merely their divisors are coprime. The divisors are integers, $t_1$ and $t_2$, such that $\phi_1/t_1$ and $\phi_2/t_2$ are primitive forms. The *product*, or *compound*, of the forms $\phi_1$ and $\phi_2$ will be defined to be the form $[a_1a_2, b_1, c_1]$, and will be denoted by $\phi_1\phi_2$. The significance of this definition lies in the fact that, when $t_1$ and $t_2$ are coprime, *it defines a unique product class.*

THEOREM 2. *Let the divisors of the classes $C_1$ and $C_2$ of discriminant $d$ be assumed coprime. Then, for all choices of united forms* (10), *the form $[a_1a_2, b_1, c_1]$ belongs to a unique class.*

PROOF. Consider, besides the forms $\phi_1$ and $\phi_2$, a second pair, $\phi_3=[a_3, b_2, a_4c_2]$ in $C_1$, $\phi_4=[a_4, b_2, a_3c_1]$ in $C_2$. It is to be proved that $\phi_1\phi_2=[a_1a_2, b_1, c_1]\sim[a_3a_4, b_2, c_2]=\phi_3\phi_4$. The difficulty in applying Lemma 2 immediately lies in the circumstance that $a_1a_2$ and $a_3a_4$ may not be coprime, and hence that it may not be possible to obtain equal middle coefficients by merely adding multiples of $2a_1a_2$ to $b_1$ and $2a_3a_4$ to $b_2$. To circumvent this difficulty, we introduce intermediate forms, with coefficients prime to both. Thus, an integer $a_5$ can be chosen, which is primitively represented by $C_1$, and such that $a_5/t_1$ is prime to $2a_1a_2a_3a_4$; and an integer $a_6$, primitively represented by $C_2$, such that $a_6/t_2$ is prime to $2a_1a_2a_3a_4a_5$. Construct $\phi_5=[a_5, b_3, c_3]$ in $C_1$, $\phi_6=[a_6, b_4, c_4]$ in $C_2$. Since $2a_1a_2$, $a_5/t_1$, and $a_6/t_2$ are coprime in pairs, an integer $b_5$ can be found to satisfy

$$(11)\quad b_5\equiv b_1 \bmod 2a_1a_2,\ b_5/t_1\equiv b_3/t_1 \bmod 2a_5/t_1,\ b_5/t_2\equiv b_4/t_2 \bmod 2a_6/t_2.$$

Then $d-b_5^2$ is divisible by each of $4a_1a_2$, $a_5/t_1$, and $a_6/t_2$, and hence

$$d-b_5^2=4a_1a_2a_5a_6c_5/t,\qquad t=t_1t_2,\quad \text{with } c_5 \text{ integral.}$$

Hence $\phi_1\sim[a_1, b_5, a_2a_5a_6c_5/t]\sim[a_5, b_5, a_1a_2a_6c_5/t]$, $\phi_1\phi_2\sim[a_1a_2, b_5, a_5a_6c_5/t]$. By Lemma 2, $\phi_1\phi_2\sim[a_5a_2, b_5, a_1a_6c_5/t]$. Similarly, since $\phi_2\sim\phi_6$, the last displayed form is equivalent to $[a_5a_6, b_5, a_1a_2c_5/t]$. We now choose an integer $b_6$ such that

$$b_6/t\equiv b_2/t \bmod 2a_3a_4/t,\qquad b_6/t\equiv b_5/t \bmod 2a_5a_6/t.$$

Then $\phi_3$, $\phi_4$, $\phi_5$, $\phi_6$, $\phi_3\phi_4$, and $\phi_5\phi_6$ are equivalent to new forms with a common middle coefficient $b_6$, respective first coefficients $a_3$, $a_4$, $a_5$, $a_6$, $a_3a_4$, $a_5a_6$; while the last coefficients are determined from $d=b_6^2-4a_3a_4a_5a_6c_6/t$, with $c_6$ an integer. By Lemma 2, $\phi_3\sim\phi_5$, $\phi_3\phi_6\sim\phi_5\phi_6$; $\phi_4\sim\phi_6$, $\phi_3\phi_4\sim\phi_3\phi_6\sim\phi_5\phi_6\sim\phi_1\phi_2$. This completes the proof.

ILLINOIS INSTITUTE OF TECHNOLOGY