Conspectus materiae tomi XX, fasciculi 3

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange	Address of the Editorial Board and of the exchange	Die Adresse der Schriftleitung und des Austausches	Адрес редакции и книгообмена
ACTA ARITHMETICA			
ul. Śniadeckich 8, Warszawa 1			

Les volumes IV et suivants sont à obtenir chez	Volumes from IV on are available at	Die Bände IV und folgende sind zu beziehen durch	Томы IV следующие можно получить через
Ars Polona-Ruch, Krakowskie Przedmieście 7, Warszawa 1			

Prix d'un fascicule	Price of an issue	Preis für ein Heft	Цена номера
	$ 4.35		

Les volumes I–III sont à obtenir chez	Volumes I–III are available at	Die Bände I–III sind zu beziehen durch	Томы I–III можно получить через
Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y,			

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XX (1972)

Composition of binary quadratic forms over integral domains

by

BILL J. DULIN (College Station, Tex.) and
H. S. BUTTS* (Baton Rouge, La.)

Introduction. There are two principal (classical) definitions of composition of binary quadratic forms over the domain Z of rational integers — that of Gauss using bilinear substitutions (see [14], Arts. 235–243 and [29], pp. 231–243), and that of Dirichlet–Dedekind using "united forms" (see [11], [26], pp. 1171–1175, [9], pp. 134–140, [10], pp. 60–79). Another method of dealing with composition is to associate with each form a module, and from this point of view composition is really just multiplication of suitable modules. (This idea seems to have been due to Dedekind; a recent paper concerned with this approach is [7].)

Two papers have recently appeared which are concerned with the problem of extending the theory of composition to various types of integral domains — in [22] Kaplansky uses the module approach to extend composition to Bezout domains (i.e. integral domains in which finitely generated ideals are principal), and in [6] Butts and Estes determine a class of domains in which "united form" composition holds and give a necessary and sufficient condition for the existence of a Gaussian compound of two primitive forms of the same discriminant.

In this paper we are concerned with Gaussian composition and "united form" composition and the relationship between them. In section 2 we consider the compound and the direct compound of Gauss, giving necessary and sufficient conditions for existence in each case, and as an application we extend the theory of Gaussian composition to Bezout domains. In section 3 we consider "united form" composition and give necessary and sufficient conditions for its existence in a G-domain (i.e. an integral domain of characteristic $\neq 2$ in which any two primitive forms of the same discriminant have a direct (Gaussian) compound). Section 4 is devoted to showing that "united form" composition holds in (and giving examples

* This author received partial support from a National Science Foundation research grant during the preparation of this paper.

of) elementary divisor domains. The two main results in section 5 are the following: (1) if D is a domain with characteristic $\neq 2$ such that finitely generated projective D-modules are free and such that $x^2 \equiv y^2 \pmod 4$ implies $x \equiv y \pmod 2$ in D, then D is a G-domain; and (2) if D is a PID, then $D[x]$ is a G-domain.

1. Some preliminaries. Let D be an integral domain (i.e. a commutative ring without proper divisors of zero and with multiplicative identity) with quotient field K, and characteristic not 2. If x, y are indeterminates over D, the polynomial $ax^2+bxy+cy^2 \in D[x, y]$ is called a *binary quadratic form* over D and will be denoted by $[a, b, c]$; we will use the conventions of [9] regarding such forms. If $f = [a, b, c]$, then the *matrix of* f is the matrix

$$F = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

with entries in K, and the *discriminant* of f is $d = b^2 - 4ac$. In this paper we are concerned only with forms having nonsquare discriminant, i.e. d is not the square of an element of K (if D is integrally closed, this is equivalent to assuming that d is not the square of an element of D — e.g. see [6], pp. 158–159).

If x_i, y_i $(i = 1, 2)$ are four different indeterminates over D and the linear transformation

$$(1) \qquad T: \begin{cases} x_1 = a_{11}x_2 + a_{12}y_2, \\ y_1 = a_{21}x_2 + a_{22}y_2, \end{cases} \quad a_{ij} \in D$$

transforms $a_1x_1^2+b_1x_1y_1+c_1y_1^2$ into $a_2x_2^2+b_2x_2y_2+c_2y_2^2$, i.e.

$$(2) \qquad \begin{aligned} a_2 &= a_1a_{11}^2 + b_1a_{11}a_{21} + c_1a_{21}^2, \\ b_2 &= 2a_1a_{11}a_{12} + b_1(a_{11}a_{22} + a_{12}a_{21}) + 2c_1a_{21}a_{22}, \\ c_2 &= a_1a_{12}^2 + b_1a_{12}a_{22} + c_1a_{22}^2 \end{aligned}$$

then we say that $f_1 = [a_1, b_1, c_1]$ is transformed into $f_2 = [a_2, b_2, c_2]$ under the linear transformation $T = (a_{ij})$. If d_i is the discriminant of f_i $(i = 1, 2)$, then a direct calculation shows that $d_2 = |T_1|^2 d_1$ where $|T|$ is the determinant of T. If F_i denotes the matrix of f_i $(i = 1, 2)$, then the matrix equation $T'F_1T = F_2$ (T' = the transpose of T) simply states that f_1 is transformed into f_2 by T, and the relation between d_1 and d_2 follows by the multiplication theorem for determinants. In case $|T| = 1$ we say that T is *unimodular* and that f_1 *is equivalent to* f_2 (in symbols, $f_1 \sim f_2$).

The *divisor* of a binary quadratic form $f = [a, b, c]$ is the ideal (a, b, c) of D generated by the coefficients of f, and f is said to be *primitive* provided the divisor of f is D.

If d is a non-square discriminant of D, then $F(d)$ will denote the set of all binary quadratic forms over D with discriminant d and $P(d)$ the set of primitive forms of discriminant d. It is clear that the relation $\sim$ defined above is an equivalence relation of $F(d)$ and on $P(d)$ (it follows easily from (2) that if $f_1 \sim f_2$ then the divisor of f_1 = the divisor of f_2); the equivalence class of a form f under $\sim$ will be denoted by $\bar{f}$.

2. Gaussian composition. Gauss ([14], Arts. 235–243) based his concept of composition on the notion of transforming a form into a product of two forms by a bilinear transformation (also, see [6]).

In general we denote the transpose of a matrix M by M', and by a bilinear transformation we mean a transformation T defined by a matrix equation of the form

$$[x_3 \ y_3]' = (a_{ij})[x_1x_2 \ x_1y_2 \ y_1x_2 \ y_1y_2]'$$

where (a_{ij}) is a 2×4 matrix with entries in D and x_i, y_i $(i = 1, 2)$ are four different indeterminates over D. If no confusion results, we frequently also denote by T the matrix (a_{ij}) of the transformation. We emphasize that the order of the x_i, y_i in the column matrix in the above equation is important, that is, T is linear in (x_1, y_1) and in (x_2, y_2).

Let $f_i = [a_i, b_i, c_i] \in F(d)$ for $i = 1, 2, 3$. We say that f_3 is *transformable into* f_1f_2 provided there exists a bilinear transformation

$$(3) \qquad T: \begin{cases} x_3 = p_0x_1x_2 + p_1x_1y_2 + p_2y_1x_2 + p_3y_1y_2, \\ y_3 = q_0x_1x_2 + q_1x_1y_2 + q_2y_1x_2 + q_3y_1y_2 \end{cases}$$

such that

$$a_3x_3^2 + b_3x_3y_3 + c_3y_3^2 = (a_1x_1^2 + b_1x_1y_1 + c_1y_1^2)(a_2x_2^2 + b_2x_2y_2 + c_2y_2^2)$$

in the polynomial domain $D[x_1, y_1, x_2, y_2]$. It is clear that if f_3 is transformable into f_1f_2, then f_3 is transformable into f_2f_1. Furthermore, if Δ_i is the divisor of f_i $(i = 1, 2, 3)$ and f_3 is transformable into f_1f_2, it is easy to check that $\Delta_1\Delta_2 \subset \Delta_3$.

If (a_{ij}) is a 2×4 matrix with entries in D, then the divisor of (a_{ij}) is the ideal of D generated by the six minor determinants of order 2 in (a_{ij}) and (a_{ij}) will be called *primitive* if its divisor is D. By the divisor of a bilinear transformation T we mean the divisor of the associated 2×4 coefficient matrix of T, and T will be called primitive if its matrix is primitive. The six minor determinants of order 2 in the matrix of the transformation in (3) play an important role in the Gaussian development and we denote them by

$$(4) \qquad D_{ij} = p_iq_j - q_ip_j \quad (0 \leqslant i < j \leqslant 3).$$

Since the transformation T in (3) is linear in (x_1, y_1) and in (x_2, y_2), it can be considered as a linear transformation

$$T_1: \begin{cases} x_3 = (p_0x_1+p_2y_1)x_2+(p_1x_1+p_3y_1)y_2, \\ y_3 = (q_0x_1+q_2y_1)x_2+(q_1x_1+q_3y_1)y_2 \end{cases} \tag{5}$$

with coefficients in $D[x_1, y_1]$, and also as a linear transformation

$$T_2: \begin{cases} x_3 = (p_0x_2+p_1y_2)x_1+(p_2x_2+p_3y_2)y_1, \\ y_3 = (q_0x_2+q_1y_2)x_1+(q_2x_2+q_3y_2)y_1 \end{cases} \tag{6}$$

with coefficients in $D[x_2, y_2]$. In general, if T is a bilinear transformation, we will denote by T_i $(i = 1, 2)$ the associated linear transformations in (5) and (6). It is clear that applying either linear transformation T_i to f_3 is equivalent to applying T to f_3. The following proposition is easy to establish.

PROPOSITION 2.1. *If T is a bilinear transformation and S is a 2×2 matrix with entries in D, then ST is the matrix of a bilinear transformation and $ST_i = (ST)_i$ for $i = 1, 2$.*

The following proposition was proved by Gauss for the case $D = Z$ (the ring of integers), but we sketch a proof for the sake of completeness.

THEOREM 2.2. *Let f_i be a form with discriminant d_i and coefficients in D $(i = 1, 2, 3)$. If f_3 is transformable into f_1f_2 under T (using the notation of (3)–(6)), then there exist $r_1, r_2 \in K$ such that the following holds:*

(a) $d_i = d_3r_i^2$ *for* $i = 1, 2$,

(b) $$\begin{cases} D_{01} = a_1r_2,\ D_{03}-D_{12} = b_1r_2,\ D_{23} = c_1r_2, \\ D_{02} = a_2r_1,\ D_{03}+D_{12} = b_2r_1,\ D_{13} = c_2r_1, \end{cases}$$

(c) $$\begin{cases} a_3r_1r_2 = q_1q_2-q_0q_3,\ c_3r_1r_2 = p_1p_2-p_0p_3, \\ b_3r_1r_2 = p_0q_3+q_0p_3-p_1q_2-q_1p_2. \end{cases}$$

Conversely, if f_1 and f_2 are given and there exist $p_i, q_i \in D$ $(i = 0, 1, 2, 3)$, $r_i \in K$ $(i = 1, 2)$ and $a_3, b_3, c_3 \in D$ such that (b) *and* (c), *then $[a_3, b_3, c_3]$ is transformable into f_1f_2 under the bilinear transformation determined by the p_i, q_i (as in* (3)) *and* (a) *holds.*

Proof. Since $f_3 = f_1f_2$ under the bilinear transformations T_i of (5) and (6), it follows that

$$d_3|T_1|^2 = f_1^2d_2 \quad \text{and} \quad d_3|T_2|^2 = f_2^2d_1 \tag{7}$$

where $|T_i|$ is the determinant of T_i. From (5) and (6) it is clear that

$$|T_1| = D_{01}x_1^2+(D_{03}-D_{12})x_1y_1+D_{23}y_1^2, \tag{8}$$

$$|T_2| = D_{02}x_2^2+(D_{03}+D_{12})x_2y_2+D_{13}y_2^2. \tag{9}$$

Now (a) and (b) follow directly by using (8) and (9) and equating coefficients in (7). To establish (c), we consider the linear transformation

$$S: x_1' = r_1f_2x_1,\ y_1' = r_1f_2y_1 \tag{10}$$

and note that

$$f_1(x_1', y_1') \overset{S}{=} r_1^2f_2f_1f_2 \overset{T_1^{-1}}{=} r_1^2f_2f_3 \tag{11}$$

so that f_1 is transformable into $r_1^2f_3f_2$ by the bilinear transformation with matrix

$$\begin{bmatrix} q_2 & q_3 & -p_2 & -p_3 \\ -q_0 & -q_1 & p_0 & p_1 \end{bmatrix} \tag{12}$$

and we can apply (a) and (b). There exist R_1, R_2 such that $d_2 = d_1R_1^2$ and $r_1^4d_3 = d_1R_2^2$, and since $d_i = d_3r_i^2$ $(i = 1, 2)$ it follows that $R_2 = \pm r_1$ and $R_1 = \pm r_2/r_1$. Applying (b) and (12) and comparing the coefficients of $x_1^2x_2^2$ in $f_3 \overset{T}{=} f_1f_2$, we find that $R_1 = -r_2/r_1$ and (c) follows. The converse follows by applying the indicated transformation to $[a_3, b_3, c_3]$ and using (b) and (c).

Remark. If f_3 and f_3' are both transformed into f_1f_2 under the same bilinear transformation T, then $f_3 = f_3'$ since the transformation T_1 in (5) has an inverse in $K(x_1, y_1)$ (it follows from (8) that $|T_1| \neq 0$). This also holds in case f_3, f_3' have coefficients in K.

PROPOSITION 2.3. *Let f_i be a binary quadratic form with coefficients in D $(i = 1, 2, 3)$ and suppose that f_3 is transformable into f_1f_2 under T. If f_3^* is taken into f_3 and f_i is taken into f_i^* $(i = 1, 2)$ by linear transformations L_i with coefficients in D $(i = 1, 2, 3)$, then f_3^* is transformable into $f_1^*f_2^*$ under the transformation*

$$M = L_3T\begin{bmatrix} s_1L_2 & u_1L_2 \\ t_1L_2 & v_1L_2 \end{bmatrix} \quad \textit{where} \quad L_1 = \begin{bmatrix} s_1 & u_1 \\ t_1 & v_1 \end{bmatrix}.$$

Proof. Let F_i, F_i^* denote the matrices of f_i, f_i^* respectively $(i = 1, 2, 3)$. Since $L_3'F_3^*L_3 = F_3$, it follows that $(L_3T_1)'F_3^*(L_3T_1) = T_1'F_3T_1 = f_1F_2$ (using the notation of (5), (6), and Proposition 2.1). Since $L_3T_1 = (L_3T)_1$, f_3^* is transformable into f_1f_2 under the bilinear transformation L_3T.

Similarly, $T_1'F_3T_1 = f_1F_2$ implies that

$$(T_1L_2)'F_3(T_1L_2) = f_1L_2'F_2L_2 = f_1F_2^*.$$

Since $T_1L_2 = S_1$ where

$$S = T\begin{bmatrix} L_2 & N \\ N & L_2 \end{bmatrix}, \quad N = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

f_3 is transformable into $f_1 f_2^*$ under S. It follows in the same manner that f_3 is transformable into $f_1^* f_2$ under the bilinear transformation

$$R = T\begin{bmatrix} s_1 I & u_1 I \\ t_1 I & v_1 I \end{bmatrix}, \qquad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

The proof is easily completed by combining the above three cases.

Remark. Since f_3 is transformable into $f_1 f_2$ under T in Proposition 2.3, there exist $r_1, r_2 \in K$ such that (a), (b), (c) of Theorem 2.2 hold. What is the effect on r_i of the application of the linear transformations L_i in Proposition 2.3? Let d_i, d_i^* denote respectively the discriminant of f_i, f_i^* for $i = 1, 2, 3$ and denote the six minor determinants of order 2 in M by D_{ij}^* $(0 \leqslant i < j \leqslant 3)$. Applying Theorem 2.2, there exist $r_1^*, r_2^* \in K$ such that (a), (b), (c) hold. Hence $d_i = d_3 r_i^2$ and $d_i^* = d_3^* (r_i^*)^2$ for $i = 1, 2$. Set $k_i = |L_i|$ for $i = 1, 2, 3$. Since $d_3 = d_3^* k_3^2$ and $d_i^* = d_i k_i^2$, we have $(r_i^*)^2 = (r_i k_i k_3)^2$ for $i = 1, 2$. Computing D_{01}^*, D_{02}^* and using (b) of Theorem 2.2, we find that $r_i^* = r_i k_i k_3$ for $i = 1, 2$.

Proposition 2.4. *If T is a 2×4 matrix over D, then there exists a 4×2 matrix S over D such that $TS = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ if and only if T is primitive.*

Proof. Let $T = (a_{ij})$ where $i = 1, 2$ and $j = 1, 2, 3, 4$. If the ideal generated by the $D_{ij} = a_{1i}a_{2j} - a_{2i}a_{1j}$ $(1 \leqslant i < j \leqslant 4)$ is D, then there exist $u_i \in D$ $(i = 1, 2, 3, 4)$ such that $\sum_{i=1}^{4} u_i a_{1i} = 1$ and $b_{ij} \in D$ $(1 \leqslant i < j \leqslant 4)$ such that $\sum b_{ij} D_{ij} = \sum_{i=1}^{4} u_i a_{2i}$.

Set $x_{11} = u_1 + b_{12}a_{12} + b_{13}a_{13} + b_{14}a_{14}$, $x_{21} = u_2 - b_{12}a_{11} + b_{23}a_{13} + b_{24}a_{14}$, $x_{31} = u_3 - b_{13}a_{11} - b_{23}a_{12} + b_{34}a_{14}$, $x_{41} = u_4 - b_{14}a_{11} - b_{24}a_{12} - b_{34}a_{13}$. Then $\sum_{i=1}^{4} x_{i1}a_{1i} = 1$ and $\sum_{i=1}^{4} x_{i1}a_{2i} = 0$. Similarly, there exist $x_{i2} \in D$ $(i = 1, \ldots, 4)$ such that $\sum_{i=1}^{4} x_{i2}a_{2i} = 1$ and $\sum_{i=1}^{4} x_{i2}a_{1i} = 0$. It follows that

$$(a_{ij})(x_{ij}) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Conversely, suppose that there is a matrix S over D such that

$$TS = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Let $W = (w_{ij})$ where $w_{1j} = a_{2j}$ and $w_{2j} = -a_{1j}$ for $j = 1, \ldots, 4$. Then $W'T = (y_{ij})$ where $y_{ii} = 0$, $y_{ij} = -D_{ij}$ for $j > i$, and $y_{ij} = D_{ji}$ for $j < i$. Since $(W'T)S = W'$, it follows that the ideal generated by the six minor determinants of order 2 in T is D and T is primitive.

The relationship between binary quadratic forms over D and certain D-modules in a quadratic extension of the quotient field K of D has been developed as a useful technique in investigating properties of forms and D-modules (e.g. see [22]; [6], pp. 173–180 and [7] for recent applications and other references). If $d = t^2 - 4n$ is a nonsquare discriminant in K then $f(x) = x^2 - tx + n$ is an irreducible polynomial in the polynomial ring $D[x]$; and the roots of $f(x)$ are $(t + \sqrt{d})/2$ and $(t - \sqrt{d})/2$ where $\sqrt{d}$ is a fixed root of $x^2 - d$ over K. For $\alpha, \beta \in K(\sqrt{d})$, $[\alpha, \beta]D = \{\alpha x + \beta y \mid x, y \in D\}$ will denote the D-module generated by α and β. If $\alpha = a + b\sqrt{d} \in K(\sqrt{d})$, then $\bar{\alpha} = a - b\sqrt{d}$ is the conjugate of α and $N(\alpha) = \alpha\bar{\alpha}$ is the norm of α. Given a D-module $M \subset K(\sqrt{d})$ the set of conjugates of elements of M is also a D-module, denoted by $\bar{M}$. We associate with a form $f = [a, b, c] \in F(d)$ the D-modules $M_f = [a, (b + \sqrt{d})/2]D$ and $\bar{M}_f = [a, (b - \sqrt{d})/2]D$, and note that $M_f = \bar{M}_f$ if and only if $b = aq$ with $q \in D$. Furthermore, with a D-module $M = [\alpha, \beta]D$ we associate a form $f_M = (\alpha x + \beta y)(\bar{\alpha} x + \bar{\beta} y) \in K[x, y]$, called the norm form of M.

Theorem 2.5. *Let $f_i = [a_i, b_i, c_i]$ be a form over D with discriminant d_i $(i = 1, 2, 3)$, and suppose that f_3 is transformable into $f_1 f_2$ by a primitive bilinear transformation T (and hence there exist $r_1, r_2 \in K$ such that $d_1 r_2^2 = d_2 r_1^2$ by Theorem 2.2). If $r_1\sqrt{d_2} = r_2\sqrt{d_1}$ then the following hold.*

(13) *There is a unique ordered pair (α_1, α_2) of independent elements in $K(\sqrt{d_1}) = K(\sqrt{d_2})$ such that the matrix equation $(a_1a_2, a_1\omega_2, a_2\omega_1, \omega_1\omega_2) = (\alpha_1, \alpha_2)T$ holds, where $\omega_i = (b_i + \sqrt{d_i})/2$ for $i = 1, 2$.*

(14) $$M_{f_1} M_{f_2} = [\alpha_1, \alpha_2]D.$$

(15) *The norm form $[\alpha_1, \alpha_2]D$ is $a_1 a_2 f_3$.*

If $r_1\sqrt{d_2} = -r_2\sqrt{d_1}$ then (13)–(15) hold with ω_2 replaced by $\bar{\omega}_2$ (or, with ω_1 replaced by $\bar{\omega}_1$).

Set

$$U = (a_1a_2, a_1\omega_2, a_2\omega_1, \omega_1\omega_2), \qquad T = \begin{bmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{bmatrix},$$

and consider the matrix equation $U = (\alpha_1, \alpha_2)T$. Since $a_1a_2 = p_0a_1 + q_0a_2$ and $a_1\omega_2 = p_1a_1 + q_1a_2$, it follows from Theorem 2.2 that

$$\alpha_1 = (a_2q_1 - q_0\omega_2)/r_2 \quad \text{and} \quad \alpha_2 = (-a_2p_1 + p_0\omega_2)/r_2.$$

Furthermore it is easy to check that α_1, α_2 satisfy $U = (\alpha_1, \alpha_2)T$. We will establish later that the D-module $[\alpha_1, \alpha_2]D$ is two dimensional.

Since $U = (\alpha_1, \alpha_2)T$, we have $M_{f_1} M_{f_2} \subset [\alpha_1, \alpha_2]D$. From Proposition 2.4 there exists a 4×2 matrix V such that $UV = (\alpha_1, \alpha_2)TV = (\alpha_1, \alpha_2)$,

and consequently $[a_1, a_2]D \subset M_{f_1}M_{f_2}$. We note that $a_1a_2, a_1\omega_2 \in [a_1, a_2]D$, which implies that a_1, a_2 are linearly independent over K.

Now, consider (15). Let x_i, y_i be indeterminates over D for $i = 1, 2$ and set

$$W = \begin{bmatrix} x_1 \cdot x_2 \\ x_1 \cdot y_2 \\ y_1 \cdot x_2 \\ y_1 \cdot y_2 \end{bmatrix} \quad \text{and} \quad TW = \begin{bmatrix} x_3 \\ y_3 \end{bmatrix}. \tag{16}$$

Since $U = (a_1, a_2)T$, we have

$$UW = (a_1, a_2)\begin{bmatrix} x_3 \\ y_3 \end{bmatrix} \tag{17}$$

and

$$(a_1x_1 + \omega_1y_1)(a_2x_2 + \omega_2y_2) = a_1x_3 + a_2y_3, \tag{18}$$

$$(a_1x_1 + \overline{\omega}_1y_1)(a_2x_2 + \overline{\omega}_2y_2) = \overline{a}_1x_3 + \overline{a}_2y_3; \tag{19}$$

multiplying (18) by (19) we obtain

$$a_1f_1 \cdot a_2f_2 = f_M \quad \text{where} \quad M = [a_1, a_2]D. \tag{20}$$

It is clear from (16)–(20) that the form $(1/a_1a_2)f_M = h$ is transformed into f_1f_2 by the bilinear transformation determined by T, i.e. the transformation $(16)_2$. Since h has coefficients in K, $h = f_3$ by the remark after Theorem 2.2 and (15) follows. If $r_1\sqrt{d_2} = -r_2\sqrt{d_1}$, then (13)–(15) follow with ω_2 replaced by $\overline{\omega}_2$ by the same argument we just completed. We note that in this second case the module M obtained in (14) is the conjugate of that obtained in the first case, and thus the norm form f_M is the same in both cases. If $r_1\sqrt{d_2} = -r_2\sqrt{d_1}$, then (13)–(15) hold with ω_1 replaced by $\overline{\omega}_1$, and the generators α_1, α_2 of the module in (14) are the same as those in the proof given above of the first case.

The following Lemma is easy to establish and we state it without proof.

LEMMA 2.6. *Let α_1, α_2 be elements of a quadratic extension $K(\sqrt{d})$ of K, and let (a_{ij}) be a 2×2 matrix with entries in D. Define a_1^*, a_2^* by the matrix equation $(\alpha_1, \alpha_2)(a_{ij}) = (a_1^*, a_2^*)$, and set $M = [\alpha_1, \alpha_2]D$, $M^* = [a_1^*, a_2^*]D$. Then the norm form f_M is transformed into the norm form f_{M^*} by the linear transformation determined by (a_{ij}).*

THEOREM 2.7. *Let f_i be a form over D of discriminant d_i for $i = 1, 2, 3$ and suppose that f_3 is transformable into f_1f_2 by two primitive bilinear transformations T, T^*. Let r_i, r_i^* be the elements of K associated by Theorem 2.2 with T, T^* respectively such that $d_i = d_3r_i^2 = d_3(r_i^*)^2$ and hence $r_i = \pm r_i^*$ for $i = 1, 2$. If $r_1r_2 = r_1^*r_2^*$, then there exists an automorph W of f_3 such that $|W| = \pm 1$ and $T^* = WT$ ($|W| = \pm 1$ according as $|T_1^*| = \pm|T_1|$, using the notation of Proposition 2.1).*

Conversely, given T as above and W an automorph of f_3, then $T^* = WT$ is a primitive bilinear transformation transforming f_3 into f_1f_2 and $r_1r_2 = r_1^*r_2^*$.

Proof. By Theorem 2.5 we can associate unique ordered pairs (a_1, a_2), (a_1^*, a_2^*) of linearly independent elements with T, T^* respectively such that $[a_1, a_2]D = M_{f_1}M_{f_2} = [a_1^*, a_2^*]D$ or $[a_1, a_2]D = M_{f_1}\overline{M}_{f_2} = [a_1^*, a_2^*]D$. In either case $[a_1, a_2]D = [a_1^*, a_2^*]D$ and there exists a 2×2 unimodular matrix W with entries in D such that the matrix equation $(a_1^*, a_2^*)W = (a_1, a_2)$ holds. Furthermore, from Theorem 2.5 we have the matrix equation $(a_1^*, a_2^*)T^* = (a_1, a_2)T$, and therefore $(a_1^*, a_2^*)T^* = (a_1^*, a_2^*)WT$, which implies that $T^* = WT$ since a_1^*, a_2^* are linearly independent over K. Again from Theorem 2.5, the norm form of $[a_1, a_2]D$ and the norm form of $[a_1^*, a_2^*]D$ are both equal to $a_1a_2f_3$, and since $(a_1^*, a_2^*)W = (a_1, a_2)$ it is clear from Lemma 2.6 that W is an automorph of f_3 (i.e. W takes f_3 into itself). Since $T^* = WT$ we have from Proposition 1 that $T_i^* = WT_i$, and (b), (8), (9) of Theorem 2.2 imply that $|W| = r_i^*/r_i$ $(i = 1, 2)$. Consequently $|W| = \pm 1$ according as $|T_1^*| = \pm|T_1|$.

Conversely, let T be given as in the Theorem and let W be an automorph of f_3. Since $|W| = \pm 1$ and T is primitive, it follows from Proposition 2.4 that $T^* = WT$ is primitive. Noting that $T_1^* = WT_1$ and denoting the matrices of f_2, f_3 by F_2, F_3 respectively, we have $(T_1^*)'F_3T_1^* = (WT_1)'F_3WT_1 = T_1'F_3T_1 = f_1F_2$ so that f_3 is transformable into f_1f_2 by T^*. Moreover, (b), (8), (9) of Theorem 2 imply that $|W| = r_i^*/r_i$ for $i = 1, 2$ and $r_1r_2 = r_1^*r_2^*$.

Remark. We first became aware of the possibility that Theorem 2.7 was valid due to a recent result of Professor Gordon Pall — he proved Theorem 2.7 for the case in which $D = Z$ (the ring of integers), f_1 and f_2 primitive forms of the same discriminant, and r_i, r_i^* positive $(i = 1, 2)$ using methods completely different from those used above. If $D = Z$ in Theorem 2.7 and $r_i \geqslant 0$ $(i = 1, 2)$, then f_3 is called a Gaussian compound (or, direct compound) of f_1f_2 (see [14] and [6], p. 155) and T is sometimes called a Gaussian substitution. As Professor Pall remarks, it is strange that this result — which asserts the essential uniqueness of the Gaussian substitution under which $f_3 = f_1f_2$ — appears nowhere in the literature, with one possible exception. The exception is that F. Arndt states without proof a result in a different form apparently equivalent to that proved by Professor Pall (see Dickson's History), and his statement is not mentioned by G. B. Mathews in his exposition of Arndt's work in his book "Theory of Numbers".

DEFINITION. Following Gauss we call f_3 a *compound* of $f_1 f_2$ provided f_3 is tranformable into $f_1 f_2$ by a *primitive* bilinear transformation. If D were an ordered domain, we could define a Gaussian compound in accordance with the original definition of Gauss as indicated in the above Remark; however, over a general domain we define the Gaussian compound only in the case that f_1 and f_2 have the same discriminant (see [5] and [6], p. 155 for remarks in this connection). If f_1 and f_2 are forms over D of the same discriminant, then f_3 is a *Gaussian compound* (or, a *direct* compound) provided f_3 is transformable into $f_1 f_2$ by a primitive bilinear transformation T such that the r_i $(i = 1, 2)$ associated with T by Theorem 2.2 are both equal to 1 (i.e. $|T_i| = f_i$ for $i = 1, 2$ in the notation of Proposition 2.1).

THEOREM 2.8. *Let $f_i = [a_i, b_i, c_i]$ be a form over D of discriminant d for $i = 1, 2$ such that $b_1 \equiv b_2 \pmod 2$ in D. If $M = M_{f_1} M_{f_2}$ is a free 2-dimensional D-module, then $(1/a_1 a_2) f_M$ is a form over D transformable into $f_1 f_2$ by a primitive bilinear transformation T such that $|T_1| f_2 = |T_2| f_1$ (i.e. the r_i associated with T by Theorem 2.2 are equal). The same statement holds if M is replaced by $N = M_{f_1} \overline{M}_{f_2}$ except that $|T_1| f_2 = -|T_2| f_1$; i.e. $r_1 = -r_2$.*

Proof. Let $M = [a_1, a_2]D$ where a_1, a_2 are linearly independent elements of $K(\sqrt{d})$, and let U denote the matrix $(a_1 a_2, a_1 \omega_2, a_2 \omega_1, \omega_1 \omega_2)$ where $\omega_i = (b_i + \sqrt{d})/2$ for $i = 1, 2$. There exists a 2×4 matrix T over D such that $U = (a_1, a_2)T$ and a 4×2 matrix V over D such that $UV = (a_1, a_2)$ since $M = [a_1, a_2]D$. Since a_1, a_2 are linearly independent and $(a_1, a_2) = UV = (a_1, a_2)TV$, it follows that T is primitive by Proposition 2.4. As in (16–(20) of Theorem 2.5, the form $h = (1/a_1 a_2) f_M$ is transformed into $f_1 f_2$ under the primitive bilinear transformation $(16)_2$ associated with T. It is clear that h has coefficients in K and we will show that the coefficients of h are in D. Now, $a_1 a_2 h = f_M$ has coefficients in $M\overline{M} = M_{f_1}\overline{M}_{f_1} M_{f_2}\overline{M}_{f_2}$, and since $M_{f_i}\overline{M}_{f_i} = a_i[a_i, b_i, c_i, \omega_i]D \subset a_i[1, \omega_i]D$, it follows that h has coefficients in $A = [1, \omega_1, \omega_2, \omega_1\omega_2]D$. However, it is easy to show that $A \cap K = D$, so that h has coefficients in D and h is a compound of $f_1 f_2$ under T. By Theorem 2.2 we have $r_1, r_2 \in K$ such that $dr_1^2 = dr_2^2$, and hence $r_1 = \pm r_2$. Using $U = (a_1, a_2)T$ together with the notation of Theorem 2.2, we have

$$(21) \qquad r_1 a_1 = a_1 q_2 - q_0 \omega_1, \quad r_2 a_1 = a_2 q_1 - q_0 \omega_2,$$

$$(22) \qquad r_1 a_2 = -a_1 p_2 + p_0 \omega_1, \quad r_2 a_2 = -a_2 p_1 + p_0 \omega_2.$$

If $r_1 = -r_2$, then adding $(21)_1$ and $(21)_2$ we get $q_0 = 0$, and similarly $p_0 = 0$ from (22), so that $a_1 = 0$ — a contradiction since d is not a square. The second case of the theorem follows in a similar manner.

We can prove Theorem 2.8 for forms of different discriminants if we assume that D is integrally closed ([31], p. 256). If $f_i = [a_i, b_i, c_i]$ is a form of discriminant d_i, $\omega_i = (b_i + \sqrt{d_i})/2$ $(i = 1, 2)$ and $M = M_{f_1} M_{f_2}$ is a free 2-dimensional D-module in $K(\sqrt{d_1}, \sqrt{d_2})$, then $K(\sqrt{d_1}, \sqrt{d_2}) = K(\sqrt{d_i})$ for $i = 1, 2$. The proof of the next theorem proceeds as that of Theorem 2.8 except for the method used in showing that $A \cap K = D$; since the elements of A are integral over D, then $A \cap K = D$ when D is an integrally closed domain. Thus we have the following theorem.

THEOREM 2.9. *If f_i is a form over the integrally closed domain D of discriminant d_i $(i = 1, 2)$ and $M = M_{f_1} M_{f_2}$ is a free 2-dimensional D-module, then $(1/a_1 a_2 f_M)$ is a form over D transformable into $f_1 f_2$ by a primitive bilinear transformation T such that $r_1\sqrt{d_2} = r_2\sqrt{d_1}$ (where r_1, r_2 are the elements of K associated with T by Theorem 2.2). The same statement holds if M is replaced by $N = M_{f_1}\overline{M}_{f_2}$ except that $r_1\sqrt{d_2} = -r_2\sqrt{d_1}$.*

Combining Theorems 2.5, 2.8, and 2.9 we obtain the following result.

THEOREM 2.10. *If f_1, f_2 are forms over an integrally closed domain D, then there exists a compound of $f_1 f_2$ if and only if either $M_{f_1} M_{f_2}$ or $M_{f_1}\overline{M}_{f_2}$ is a free 2-dimensional D-module. The same statement holds over any domain D (characteristic $\neq 2$) provided f_1, f_2 have the same discriminant and their middle coefficients are congruent* mod 2 *in D.*

In the next theorem we obtain a mild extension of Theorem 5.3 of [6], p. 175. Recall that the divisor of a form is the ideal generated by its coefficients in D.

THEOREM 2.11. *If $f_i = [a_i, b_i, c_i]$ is a form over D of divisor Δ_1 and discriminant d for $i = 1, 2$, then the following are equivalent.*

(a) *There exists a Gaussian compound of $f_1 f_2$ over D.*

(b) *$M_{f_1} M_{f_2}$ is generated by two elements as a D-module, $b_1 \equiv b_2 \pmod 2$, and $\Delta_1 + \Delta_2 = D$.*

(c) *$M_{f_1} M_{f_2}$ is a free D-module, $b_1 \equiv b_2 \pmod 2$, and $\Delta_1 + \Delta_2 = D$.*

(d) *$M_{f_1} M_{f_2}$ is a free 2-dimensional D-module, $b_1 \equiv b_2 \pmod 2$, and $\Delta_1 + \Delta_2 = D$.*

Proof. (a) $\Rightarrow$ (b). The first two parts of (b) follow directly from Theorem 2.5 and (b) of Theorem 2.2 since $r_1 = r_2 = 1$ and $d_1 = d_2 = d$. Let P be a prime ideal of D such that $P \supset \Delta_1 + \Delta_2$. Since $a_1, a_2 \in P$, from part (b) of Theorem 2.2 we have $p_0 q_1 \equiv q_0 p_1 \pmod P$, $p_0 q_2 \equiv q_0 p_2 \pmod P$ and therefore

$$(23) \qquad p_0 q_1 p_2 \equiv p_0 q_2 p_1 \pmod P \quad \text{and} \quad q_0 p_1 q_2 \equiv q_0 q_1 p_2 \pmod P.$$

Furthermore $D_{03} - D_{12} = b_1 \in P$ so that

$$(24) \qquad p_0 q_3 - q_0 p_3 \equiv p_1 q_2 - q_1 p_2 \pmod P.$$

If $p_0, q_0 \notin P$ then $D_{12}, D_{03} \in P$ from (24); if one of $p_0, q_0 \in P$, then $D_{12} \in P$ from (23) and hence $D_{03} \in P$. Consequently $D_{ij} \in P$ for $0 \leqslant i < j \leqslant 3$ and $P = D$ since the transformation associated with the compound is primitive.

(b) $\Rightarrow$ (c). This is clear since $M_{f_1} M_{f_2}$ contains $a_1 a_2$ and $a_1(b_2+\sqrt{d})/2$ which are linearly independent over K.

(c) $\Rightarrow$ (d). Since $M_{f_1} M_{f_2}$ contains two linearly independent elements over K and is contained in the two dimensional vector space $K(\sqrt{d})$ over K, $M_{f_1} M_{f_2}$ must have a free basis of two elements.

(d) $\Rightarrow$ (a). By Theorem 2.8 there exists a compound $f_3 = [a_3, b_3, c_3]$ which is transformable into $f_1 f_2$ by a primitive bilinear transformation T such that $|T_1| f_2 = |T_2| f_1$, i.e. the r_i associated with T by Theorem 2.2 are equal — say $r_1 = r_2 = r$. Parts (b), (c) of Theorem 2.2 implies that rf_i is a form with coefficients in D for $i = 1, 2$ and furthermore $r^2 f_3$ is a Gaussian compound of $rf_1 \cdot rf_2$ under T. By the proof of (a) $\Rightarrow$ (b) the sum of the divisors of rf_1 and rf_2 is equal to D and there exist $x_i \in D$ $(i = 1, \ldots, 6)$ such that

$$ra_1x_1 + rb_1x_2 + rc_1x_3 + ra_2x_4 + rb_2x_5 + rc_2x_6 = 1. \tag{25}$$

Since $\Delta_1 + \Delta_2 = D$, there exist $y_i \in D$ $(i = 1, \ldots, 6)$ such that

$$a_1y_1 + b_1y_2 + c_1y_3 + a_2y_4 + b_2y_5 + c_2y_6 = 1. \tag{26}$$

Multiplying (26) by r we see that $r \in D$, and (25) implies that r is a unit of D. Denote by T^* the transformation obtained from T by replacing the q_i in the 2nd row of T by q_i/r, and let $f_3^* = [a_3, rb_3, r^2c_3]$. Then f_3^* is a Gaussian compound of $f_1 f_2$ under the primitive bilinear transformation T^*.

A Bezout domain is an integral domain with identity in which every finitely generated ideal is principal (see [4], [17] for a treatment of Bezout domains). Composition of forms over a Bezout domain has been investigated recently in [22], where composition is interpreted as multiplication of suitable modules, and in [5], using the classical approach of Gauss.

LEMMA 2.12. *The following statements hold in a Bezout domain D.*

(a) *D is integrally closed.*

(b) *Finitely generated torsion-free D-modules are free.*

(c) *$x^2 \equiv y^2 \pmod 4$ in D implies $x \equiv y \pmod 2$ in D.*

Proof. See [4] or [17] for a proof of (a), and we obtain (c) from (a) as follows. If $x^2 \equiv y^2 \pmod 4$ and characteristic $D \neq 2$, then $x^2 - y^2 - 4k = 0$ for $k \in D$; hence $(x-y)/2$ satisfies the equation $X^2 + yX - k = 0$ and $(x-y)/2 \in D$ since D is integrally closed. If D is of characteristic 2 (not considered in this paper) then it is clear that $x \equiv y \pmod 2$. Now, consider (b). An integral domain D is semi-hereditary if and only if every

finitely generated nonzero ideal of D is invertible ([8], p. 133), and therefore a Bezout domain is semi-hereditary. If D is a domain, then every finitely generated torsion-free D-module admits a monomorphism into a free module with a finite base ([8], p. 131). If D is semi-hereditary then each finitely generated submodule of a free D-module is the direct sum of a finite number of modules each of which is isomorphic with a finitely generated ideal of D ([8], p. 14). Since D and a nonzero principal ideal of D are isomorphic as D-modules, it follows that if D is a Bozout domain then each finitely generated torsion-free D-module is isomorphic to a direct sum of a finite number of copies of D and hence is a free module.

COROLLARY 2.13. *If f_i is a form of (non-square) discriminant d_i $(i = 1, 2)$ over a Bezout domain D, then there exists a compound of $f_1 f_2$ over D if and only if there exists $s \in K$ such that $d_1 = d_2 s^2$.*

Proof. If $d_1 = d_2 s^2$, then $K(\sqrt{d_1}) = K(\sqrt{d_2})$ and $M = M_{f_1} M_{f_2}$ is contained in a 2-dimensional vector space over K. However, M is a free D-module by Lemma 2.12 and M contains the elements $a_1 a_2$ and $a_1(b_2+\sqrt{d_2})/2$ which are linearly independent over K. Consequently M is a free 2-dimensional D-module and there exists a compound for $f_1 f_2$ over D by Theorem 2.10. The converse follows from Theorem 2.2.

COROLLARY 2.14. *If f_i is a form of divisor Δ_i $(i = 1, 2)$ and (non-square) discriminant d over a Bezout domain D, then there exists a Gaussian compound of $f_1 f_2$ over D if and only if $\Delta_1 + \Delta_2 = D$.*

Proof. If $\Delta_1 + \Delta_2 = D$, then a Gaussian compound of $f_1 f_2$ exists by Theorem 2.11 since $M_{f_1} M_{f_2}$ is a free 2-dimensional D-module (as in the proof of Corollary 2.13) and $b_1 \equiv b_2 \pmod 2$ by Lemma 2.12. The converse follows from Theorem 2.11.

The proof given by Gauss in [14], Art. 234 for $D = Z$ (the ring of integers) establishes the following result over a general domain.

LEMMA 2.15. *Let (a_{ij}) and (a'_{ij}) be two 2×4 matrices with entries from a domain D and set $D_{ij} = a_{1i}a_{2j} - a_{2i}a_{1j}$, $D'_{ij} = a'_{1i}a'_{2j} - a'_{2i}a'_{1j}$ for $1 \leqslant i < j \leqslant 4$. If (a_{ij}) has divisor (k) and $D_{ij} = kD'_{ij}$ for $1 \leqslant i < j \leqslant 4$, then there exists a 2×2 matrix H with entries in D such that $(a_{ij}) = H(a'_{ij})$ and $|H| = k$.*

We observe in Lemma 2.15 that in the presence of $D_{ij} = kD'_{ij}$, (a_{ij}) is of divisor (k) if and only if (a'_{ij}) is primitive. In the following Proposition D is any domain (Char. $\neq 2$) and d is not a square in K.

PROPOSITION 2.16. *Suppose $f_i, f_i^* \in F(d)$ $(i = 1, 2, 3)$, f_3 is a Gaussian compound of $f_1 f_2$ under a bilinear transformation T, f_3^* is a Gaussian compound of $f_1^* f_2^*$ under T^*, and that $f_i \sim f_i^*$ for $i = 1, 2$. Then $f_3 \sim f_3^*$; and if f is transformed into f_3 by a unimodular linear transformation L, then f is a Gaussian compound of $f_1 f_2$ under LT.*

Furthermore, if f_i is transformed into f_i^* by the unimodular linear transformation L_i $(i = 1, 2, 3)$, then f_3^* is a Gaussian compound of $f_1^* f_2^*$ under the bilinear transformation

$$S = L_3^{-1} T \begin{bmatrix} r_1 L_2 & u_1 L_2 \\ s_1 L_2 & v_1 L_2 \end{bmatrix} \quad \text{where} \quad L_1 = \begin{bmatrix} r_1 & u_1 \\ s_1 & v_1 \end{bmatrix};$$

consequently $S = WT^*$ where W is a unimodular automorph of f_3^*.

Proof. Suppose $f_i \sim f_i^*$ under $f_i \xrightarrow{L_i} f_i^*$ for $i = 1, 2$. By Proposition 2.3 f_3 is transformable into $f_1^* f_2^*$ by the bilinear transformation

$$B = T \begin{bmatrix} r_1 L_2 & u_1 L_2 \\ s_1 L_2 & v_1 L_2 \end{bmatrix} \quad \text{where} \quad L_1 = \begin{bmatrix} r_1 & u_1 \\ s_1 & v_1 \end{bmatrix}.$$

If β_{ij}, D_{ij}^* $(0 \leqslant i < j \leqslant 3)$ denote the 2×2 subdeterminants of B, T^* respectively, then it follows from the remark after Proposition 2.3 and from part (b) of Theorem 2.2 that $\beta_{ij} = D_{ij}^*$ $(0 \leqslant i < j \leqslant 3)$, and B is primitive since T^* is primitive. In view of Lemma 2.15 there exists a 2×2 matrix H with entries in D such that $B = HT^*$ and $|H| = 1$. Denoting the matrix of f_3, f_3^* by F_3, F_3^* and recalling that f_3, f_3^* is transformable into $f_1^* f_2^*$ by B, T^* respectively, we have by Proposition 1.1

$$(T_1^*)' F_3 T_1^* = B_1' F_3 B_1 = (T_1^*)' H' F_3 H T_1^*$$

and therefore $F_3^* = H' F_3 H$ — i.e. $f_3 \sim f_3^*$ under H.

Now, f_i is transformed into $f_1 f_2$ under LT by Proposition 2.3, LT is primitive and f is a Gaussian compound of $f_1 f_2$ under LT by the remark after Proposition 2.3 and by (b) of Theorem 2.2. Similarly, f_3^* is a Gaussian compound of $f_1^* f_2^*$ under S and Theorem 2.7 implies that $S = WT^*$ where W is a unimodular automorph of f_3^*.

Definition. If $f_i \in F(d)$ $(i = 1, 2, 3)$ and f_3 is a Gaussian compound of $f_1 f_2$ then we define the *compound of the classes* $\bar{f}_1, \bar{f}_2$ to be $\bar{f}_3 = \bar{f}_1 \bar{f}_2$ (and we say that $\bar{f}_3$ is determined by *composition* from $\bar{f}_1$ and $\bar{f}_2$. We denote by G_d the collection of equivalence classes determined by the equivalence relation $\sim$ on $P(d)$, and we say that D is a G-domain (or, has property G) provided any two primitive forms over D with equal discriminants have a direct compound. It is clear that a Bezout domain is a G-domain. It follows from Proposition 2.16 that composition of classes of forms of the same discriminant d is well defined, and it is clear that this operation is commutative; moreover, the operation of composition is associative (see [14], Art. 240). In addition if $d = b^2 - 4ac = b_1^2 - 4a_1 c_1$, then $[1, b, ac] = [1, b_1, a_1 c_1]$ and $[a, b, c]$ is a Gaussian compound of $[a, b, c] \cdot [1, b, ac]$ under the transformation

$$\begin{bmatrix} 1 & 0 & 0 & -c \\ 0 & 1 & a & b \end{bmatrix}.$$

Hence the classes of discriminant d determined by $\sim$ on $F(d)$ form an Abelian semi-group with identity when the compound exists, as in the case of forms with coprime divisors in a Bezout domain. Furthermore, it is easy to show that G_d is an Abelian group provided the compound exists, again as in the case of a Bezout domain. We remark that an example is given in [6], p. 177, of a Noetherian, 2-dimensional, unique factorization domain D which is not a G-domain; in fact, there is a primitive form f over D such that no Gaussian compound exists for ff.

3. United forms. Composition of binary quadratic forms in the tradition of Dirichlet and Dedekind is called *composition by "united forms"*. Two forms are called *united* if they have coprime divisors and the following configuration:

$$f = [a, b, a'c], \quad g = [a', b, ac] \quad a, a', b, c \in D.$$

It is easily checked that $h = [aa', b, c]$ is a direct compound of the united forms $f = [a, b, a'c]$ and $g = [a', b, ac]$ under the primitive bilinear transformation

$$T = \begin{bmatrix} 1 & 0 & 0 & -c \\ 0 & a & a' & b \end{bmatrix}. \tag{27}$$

As in the case of Gaussian composition, the class $\bar{h}$ is called the *compound* of the classes $\bar{f}$ and $\bar{g}$ (or, $\bar{h}$ is said to be obtained from $\bar{f}, \bar{g}$ by composition). If h' is a Gaussian compound of the united forms f', g' where $f' \in \bar{f}$ and $g' \in \bar{g}$, then it is clear that $\bar{h} = \bar{h}'$ by Proposition 2.16. Hence the compound $\bar{h}$ is independent of the united forms chosen as representatives from $\bar{f}$ and $\bar{g}$; furthermore the compound $\bar{h}$ obtained by united forms is the same as that obtained by the Gauss method.

Definition. A domain D is called a *D-domain* (or, is said *to have property D*) provided the following holds: if C_1 and C_2 are any two classes of primitive forms over D of the same discriminant, then there exist united forms f, g such that $f \in C_1$, $g \in C_2$.

Theorem 3.1. *If D is a domain in which every nonzero element is contained in a finite number of maximal ideals and such that $x^2 \equiv y^2 \pmod 4$ implies $x \equiv y \pmod 2$ in D, then D is a D-domain.*

Proof. See [6], p. 162.

Corollary 3.2. *A Dedekind domain is a D-domain. (In particular, the ring of integers is a D-domain.)*

Proposition 3.3. *If D is a D-domain, then D is a G-domain.*

Proof. If $f, g \in P(d)$, then there exist united forms f', g' such that $f' \in \bar{f}, g' \in \bar{g}$. There exists a direct compound h' of $f'g'$ (see the comment following the definition of united forms), and it follows by Proposition 2.16 that h' is a direct compound of fg.

Remark. We do not know if the converse to the above theorem is true or not.

Remark. The origin of the concept of united forms is usually attributed to either Dedekind or Dirichlet ([6], p. 156; [7], p. 24; [22]; [10], p. 66; [26]). In treating composition in [9] Dickson used the "united from" approach, and this seems to have been the accepted procedure since the time of Dedekind for quadratic forms over the integers. The reason for the rather general acceptance of the united form method of composition seems to be the following: for forms with integral coefficients, a fairly easy method can be derived for producing united forms in given classes (see [9] and [26]), and with united forms the direct compound is obtained immediately. Two comments seem to be in order: first, a rather careful reading of [14], Arts. 168, 228, 242–244, indicates that Gauss must have been essentially aware of the technique of united forms and used it in working with examples; and second, the Gauss algorithm as used by Gauss in [14], Arts. 242–244, seems to be as easy to use as the method of computing united forms.

The following two lemmas are proved in [9], p. 134.

LEMMA 3.4. *Let $m \in D$ and $t_i, q_i \in D$ for $i = 1, \ldots, n$. If $(m, t_1, \ldots, t_n) = D$ and $t_r q_s - q_r t_s \in mD$ $(r, s = 1, \ldots, n)$, then there exists $B \in D$ unique modulo (m) such that $t_i B \equiv q_i \pmod m$ for $i = 1, \ldots, n$.*

LEMMA 3.5. *Suppose $d, a_i, b_i \in D$, $b_i^2 \equiv d \pmod{4a_i}$ $(i = 1, 2)$, $b_1 \equiv b_2 \pmod 2$, and $(a_1, a_2, (b_1+b_2)/2) = D$. Then there exists $B \in D$ unique mod $2a_1a_2$ such that $B \equiv b_i \pmod{2a_i}$ for $i = 1, 2$ and $B^2 \equiv d \pmod{4a_1a_2}$. Furthermore, $(a_1, a_2, B) = D$.*

The next Lemma follows by a direct calculation.

LEMMA 3.6. *Let V, $U = (u_{ij})$, $W = (w_{ij})$ be 2×2 matrices and $T = (t_{ij})$ a 2×4 matrix with entries in D. Then the matrix equation*

$$V\left(w_{i1}\begin{bmatrix} t_{11} & t_{12} \\ t_{13} & t_{14} \end{bmatrix} + w_{i2}\begin{bmatrix} t_{21} & t_{22} \\ t_{23} & t_{24} \end{bmatrix}\right)V = \begin{bmatrix} a_{i1} & a_{i2} \\ a_{i3} & a_{i4} \end{bmatrix}$$

holds for $i = 1, 2$ if and only if

$$WT\begin{bmatrix} u_{11}V & u_{21}V \\ u_{12}V & u_{22}V \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \end{bmatrix};$$

note that U' is displayed in the last equation.

THEOREM 3.7. *The following statements are equivalent in a G-domain D.*

(a) *D is a D-domain.*

(b) *If $g_i \in P(d)$, then there exists $f_i = [a_i, b_i, c_i] \in P(d)$ such that $f_i \sim g_i$ for $i = 1, 2$ and $(a_1, a_2, (b_1+b_2)/2) = D$.*

(c) *If $f_i \in P(d)$ $(i = 1, 2)$, then there exist g_i such that $g_i \sim f_i$ for $i = 1, 2$ and g_3 is a Gaussian compound of g_1g_2 under a transformation T of the form*

$$T = \begin{bmatrix} 1 & 0 & 0 & v \\ 0 & r & s & u \end{bmatrix}.$$

(d) *If $f_i \in P(d)$ for $i = 1, 2, 3$ and f_3 is a Gaussian compound of f_1f_2 under T, then there exist 2×2 unimodular matrices $U = (u_{ij})$, V, W over D and $r, s, u, v \in D$ such that*

$$WT\begin{bmatrix} u_{11}V & u_{12}V \\ u_{21}V & u_{22}V \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & v \\ 0 & r & s & u \end{bmatrix}. \tag{28}$$

(e) *If $f_i \in P(d)$ for $i = 1, 2, 3$ and f_3 is a Gaussian compound of f_1f_2 under $T = (t_{ij})$, then there exist $a_i, b_i \in D$ $(i = 1, 2)$, 2×2 unimodular matrices U, V over D, such that $(a_1, b_1) = D$, $a_2 | b_2, b_2 \neq 0$ and*

$$U\left(a_1\begin{bmatrix} t_{11} & t_{12} \\ t_{13} & t_{14} \end{bmatrix} + b_1\begin{bmatrix} t_{21} & t_{22} \\ t_{23} & t_{24} \end{bmatrix}\right)V = \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix}. \tag{29}$$

Proof. (a) $\Rightarrow$ (b). Since D is a D-domain, there exist united forms $[a_1, b, a_2c] \sim g_1$, $[a_2, b, a_1c] \sim g_2$ and $(a_1, a_2, b) = D$ since the forms involved are primitive.

(b) $\Rightarrow$ (c). Since D is a G-domain it follows from Theorem 2.2 that two primitive forms of the same discriminant have middle coefficients congruent mod 2. Suppose $f_i = [a_i, b_i, c_i] \in P(d)$ $(i = 1, 2)$ and $(a_1, a_2, (b_1+b_2)/2) = D$. By Lemma 3.5 there exist $b, c, h, k \in D$ such that $b^2 - d = 4a_1a_2c$, $b = b_1 + 2a_1h$, $b = b_2 + 2a_2k$. Therefore $f_1 \sim [a_1, b, a_1h^2 + b_1h + c_1] = [a_1, b, a_2c] = g_1$, $f_2 \sim [a_2, b, a_1c] = g_2$, and $[a_1a_2, b, c]$ is a direct compound of g_1g_2 under a transformation as in (27).

(c) $\Rightarrow$ (d). Immediate from Proposition 2.16.

(d) $\Rightarrow$ (e). We have 2×2 unimodular matrices U, V, W over D and $r, s, u, v \in D$ such that (28) holds, so that (29) follows from Lemma 3.6 with $a_2 = 1$, $b_2 = v$, $a_1 = w_{11}$, and $b_1 = w_{12}$. Since W is unimodular, we have $(a_1, b_1) = D$. Applying W^{-1} to f_3 and the linear transformations U', V to f_1, f_2 respectively, we obtain equivalent forms $f_i^* \sim f_i$ for $i = 1, 2, 3$. It is clear from Proposition 2.16 that f_3^* is a direct compound of $f_1^*f_2^*$ under the transformation in (28), and from part (b) of Theorem 2.2 we have $v \neq 0$ since the discriminant is not a square.

(e) $\Rightarrow$ (a). If $f_i \in P(d)$ $(i = 1, 2)$ then there exists $f_3 \in P(d)$ such that f_3 is a Gaussian compound of f_1f_2 under a bilinear transformation $T = (t_{ij})$, and we have $a_i, b_i \in D$ $(i = 1, 2)$ and 2×2 unimodular matrices U, V over D such that (29) holds with $(a_1, b_1) = D$ and $a_2 | b_2 \neq 0$. We have $r, s \in D$

such that $a_1 r - b_1 s = 1$, and we define $q_i \epsilon D$ for $i = 0, \ldots, 3$ by the matrix equation

$$U\left(s\begin{bmatrix} t_{11} & t_{12} \\ t_{13} & t_{14} \end{bmatrix} + r\begin{bmatrix} t_{11} & t_{12} \\ t_{13} & t_{14} \end{bmatrix}\right) V = \begin{bmatrix} q_0 & q_1 \\ q_2 & q_3 \end{bmatrix}. \tag{30}$$

Applying Lemma 3.6, we obtain the bilinear transformation S from (29) and (30)

$$S = WT\begin{bmatrix} u_{11}V & u_{21}V \\ u_{12}V & u_{22}V \end{bmatrix} = \begin{bmatrix} a_2 & 0 & 0 & b_2 \\ q_0 & q_1 & q_2 & q_3 \end{bmatrix} \tag{31}$$

where $U = (u_{ij})$, U' is displayed in (31), and W has (a_1, b_1) and (s, r) as first and second rows respectively. Since T is primitive and U, V, W are unimodular, it follows from Theorem 2.2 and the remark after Proposition 2.3 that S is primitive; consequently a_2 is a unit in D since $a_2 | b_2$.

Define T^* *by*

$$T^* = \begin{bmatrix} 1 & 0 \\ -a_2 q_0 & 1 \end{bmatrix}\begin{bmatrix} a_2^{-1} & 0 \\ 0 & a_2 \end{bmatrix} S = \begin{bmatrix} 1 & 0 & 0 & b_2 a_2^{-1} \\ 0 & a_2 q_1 & a_2 q_0 & a_2 q_3 - b_2 q_0 \end{bmatrix}.$$

As in the proof of (d) $\Rightarrow$ (e), there exist f_i^* such that $f_i^* \sim f_i$ $(i = 1, 2, 3)$ and f_3^* is a Gaussian compound of $f_1^* f_2^*$ under T^*; furthermore,

$$f_1^* = [a_2 q_1, a_2 q_3 - b_2 q_0, -a_2 q_2 b_2 a_2^{-1}], \quad f_2^* = [a_2 q_2, a_2 q_3 - b_2 q_0, -a_2 q_1 b_2 a_2^{-1}]$$

and f_1^*, f_2^* are united forms.

If $C = \{D_\alpha\}_{\alpha \epsilon A}$ is a collection of sets, then we say that C is a *net* provided any two members of C are contained in a third member of C. The following result is easy to establish and we state it without proof.

PROPOSITION 3.8. *If D_α $(\alpha \epsilon A$, an index set$)$ and $D = \bigcup_{\alpha \epsilon A} D_\alpha$ are domains such that $\{D_\alpha\}_{\alpha \epsilon A}$ is a net and each D_α is a G-domain (D-domain), then D is a G-domain (D-domain).*

4. Elementary divisor and Bezout domains. In this section we examine some conditions under which a Bezout domain is a D-domain. We have been unable to show that every Bezout domain is a D-domain. Every example of a Bezout domain of which we are aware is not only a D-domain, but is in fact an elementary divisor ring.

DEFINITION. A ring R with the property that every matrix can, by multiplication with matrices of unit determinant, be reduced to a diagonal matrix (i.e., one having only 0 off the main diagonal) such that each element of the main diagonal divides the one to its lower right is called an *elementary divisor ring*.

In [21], pp. 471–472, it is shown that in a commutative ring, if all 1×2, 2×1, and 2×2 matrices can be diagonalized as in the above definition, then the ring is an elementary divisor ring. It is easy to see that all 1×2 and 2×1 matrices over a Bezout domain can be diagonalized by multiplying by unimodular matrices, but it is not clear that this applies to 2×2 matrices. However it follows easily that if a 2×2 matrix can be diagonalized by multiplying by unit-modular matrices, then the diagonalization can be realized by multiplying by unimodular matrices. Kaplansky [21], p. 472, shows that if all of the divisors of zero of a ring R are in the radical of R then R is an elementary divisor ring if and only if

(32) (a) each finitely generated ideal of R is principal, and
(b) $(a, b, c) = R$ implies that there exist $p, q \epsilon R$ such that $(pa, pb + qc) = R$.

An elementary divisor *domain* then is a Bezout domain in which (b) of (32) holds.

THEOREM 4.1. *If D is an elementary divisor domain, then D is a D-domain.*

Proof. If $f_i \epsilon P(d)$ for $i = 1, 2$, then Corollary 2.14 yields a direct compound of f_3 of $f_1 f_2$ under a bilinear transformation $T = (t_{ij})$. There exist unimodular matrices U, V over D and $h, k \epsilon D$ such that

$$U\begin{bmatrix} t_{11} & t_{12} \\ t_{13} & t_{14} \end{bmatrix} V = \begin{bmatrix} h & 0 \\ 0 & k \end{bmatrix}, \quad h | k. \tag{33}$$

Since $-hk = t_{12}t_{13} - t_{11}t_{14}$ is the third coefficient of f_3 by Theorem 2.2 and d is not a square, then $k \neq 0$. We note that (33) is a special case of (29), with $a_1 = 1$ and $b_1 = 0$ and the conclusion follows from (e) of Theorem 3.7.

PROPOSITION 4.2. *A Bezout domain D is a D-domain if and only if for any two forms $f, g \epsilon P(d)$ there exist $f_1 \epsilon \bar{f}$ and $f_2 \epsilon \bar{g}$ such that f_1 and f_2 have the same middle coefficients.*

Proof. Suppose $f_1 \epsilon \bar{f}, f_2 \epsilon \bar{g}$ with $f_1 = [a, b, c]$ and $f_2 = [a', b, c']$. We now appeal to the algorithm of Gauss as developed in [14], Art. 236, for forms with integral coefficients and extended in [5], Theorem 8, to Bezout domains. Taking $r_1 = r_2 = 1$, $d_1 = d_2 = d$, $Q_1 = 1$, and $Q_0 = Q_2 = Q_3 = 0$ in Theorem 8 of [5] and setting $(a, c') = (e)$, we find that the form

$$f_3 = [ac'/2, -b(kc' + ha)/e, hkb^2 + e^2 a'/a] \tag{34}$$

is a Gaussian compound of $f_1 f_2$ under the bilinear transformation

$$T = \begin{bmatrix} kb & -e & -ea'/a & -hb \\ a/e & 0 & 0 & -c'/e \end{bmatrix}$$

where h, k are elements of D such that $ha - kc' = e$; in fact, it is easy to check that f_3 is a Gaussian compound of $f_1 f_2$ by using Theorem 2.2.

In order to simplify notation, denote the form f_3 in (34) by $f_3 = [a_3, b_3, c_3]$. Now $f_3 \sim f_3^* = [c_3, -b_3, a_3]$ and f_3^* is a Gaussian compound of $f_1 f_2$ under

$$T^* = \begin{bmatrix} a/e & 0 & 0 & -c'/e \\ -kb & e & ea'/a & hb \end{bmatrix}.$$

Since

$$\begin{bmatrix} 1 & 1 \\ kc'/e & 1+(kc'/e) \end{bmatrix}\begin{bmatrix} a/e & 0 \\ 0 & -c'/e \end{bmatrix}\begin{bmatrix} h & c'/e \\ k & a/e \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -ac'/e^2 \end{bmatrix},$$

it follows from (e) of Theorem 3.7 (with $a_1 = 1$, $b_1 = 0$) that D is a D-domain. The converse is obvious.

COROLLARY 4.3. *A Bezout domain is a D-domain if and only if for any two forms $f_1', f_2' \in P(d)$ there exists $f_i = [a_i, b_i, c_i] \sim f_i'$ for $i = 1, 2$ such that $b_1 = -b_2$.*

Proof. Use Proposition 4.2 and $[a_2, b_2, c_2] \sim [c_2, -b_2, a_2]$

COROLLARY 4.4. *If D is a Bezout domain, then united form composition holds for any primitive class with itself.*

Proof. If $f \in P(d)$, then the proof of Proposition 4.2 together with that of (e) $\Rightarrow$ (a) in Theorem 3.7 shows how to find united forms $f_1, f_2 \in \bar{f}$.

We say that $f = [a, b, c] \in P(d)$ represents $n \in D$ primitively provided there exist $r, s \in D$ such that $ar^2 + brs + cs^2 = n$ and $(r, s) = D$. If f represents n primitively, then it is easy to see that f is equivalent to a form with first coefficient n (e.g. see [9]), and also to a form with last coefficient n.

PROPOSITION 4.5. *A Bezout domain is a D-domain if and only if for any two forms $f, g \in P(d)$ one represents primitively an element of D which divides an element of D that is represented primitively by the other.*

Proof. We can assume $f = [at, b, c]$ and $g = [a, b', c']$. We apply the algorithm of Gauss as in Proposition 4.2 (with $Q_0 = -1, Q_i = 0$ for $i = 1, 2, 3$) and find that the form

$$f_3 = [ta^2/e^2,\ b_1 - 2actk/e,\ hce + cc'k^2 - chk(b-b')/2]$$

is a direct compound of $f_1 f_2$ under

$$T = \begin{bmatrix} e & kc' - h(b-b')/2 & kc & -hc \\ 0 & at/e & a/e & (b+b')/2e \end{bmatrix}$$

where $\left(a, (b+b')/2\right) = (e)$ and $ha + k(b+b')/2 = e$; of course this may be checked directly by Theorem 2.2. Setting $B = (b+b')/2e$ and noting that

$$\begin{bmatrix} 0 & 1 \\ -1 & kat/e \end{bmatrix}\begin{bmatrix} 0 & at/e \\ a/e & B \end{bmatrix}\begin{bmatrix} h & -B \\ k & a/e \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -ta^2/e^2 \end{bmatrix}$$

we complete the proof as in the case of Proposition 4.2.

PROPOSITION 4.6. *If D is a domain and $f_i = [a_i, b_i, c_i]$ $(i = 1, 2)$ are elements of $P(d)$ such that $(a_1, a_2) = D$, then there exist $f_i' \in \bar{f}_i$ $(i = 1, 2)$ such that f_1' and f_2' are united.*

Proof. See [6], p. 162, for proof.

We now give several nontrivial examples (i.e. not PID's) of Bezout domains that are elementary divisor domains (denoted EDDs). We have been unable to find a Bezout domain that is not an EDD. Examples of rings that are not domains, that are not elementary divisor rings, and that are rings with the property that finitely generated ideals are principal have been given in [16], p. 378. These examples modulo a prime ideal, however, are EDDs.

If D is a Bezout domain with quotient field K and J is a domain such that $D \subset J \subset K$, then it is easy to show that J is also a Bezout domain. Furthermore, if P is a prime ideal in a Bezout domain, then D/P is a Bezout domain. If $\{D_\alpha\}_{\alpha \in \mathcal{A}}$ is a net of Bezout domains D_α, then $D = \bigcup_{\alpha \in \mathcal{A}} D_\alpha$ is a Bezout domain. However, the polynomial ring $D[x]$ is a Prüfer domain if and only if D is a field, as the following easy argument shows (D is a Prüfer domain provided every finitely generated ideal is invertible; hence a Bezout domain is Prüfer [17], p. 253–386). Suppose $D[x]$ is a Prüfer domain and let $0 \neq d \in D$. Then (d, x) is invertible and $(d, x) > (x)$ implies that $(d, x)Q = (x)$ for some ideal Q of $D[x]$. Since (x) is prime, then $Q = (x)$, $(d, x) = D[x]$, and d is a unit of D.

If D is an EDD with quotient field K and J is a domain such that $D \subset J \subset K$, then J is an EDD; we see this as follows. Let $a = a/b \in J$ with $a, b \in D$. Then $(a, b) = (d)$, $a = a_1 d$, $b = b_1 d$, $a_1 x + b_1 y = 1$ (all elements in D). Hence $(a_1 x/b_1) + y = 1/b_1 \in J$; thus, if $a \in J$, then $a = a_1/b_1$ with $a_1, b_1 \in D$ and b_1 a unit in J. It now follows readily that 2×2 matrices over J can be diagonalized. Furthermore, it is clear that if P is a prime ideal in an EDD J, then J/P is an EDD; and the union of a family of EDDs forming a net (as for Bezout domains above) is an EDD.

EXAMPLE 1. The ring D of algebraic integers is an EDD. If $(a, b, c) = D$, then there exist $a_1, b_1, c_1 \in D$ such that $aa_1 + bb_1 + cc_1 = 1$. Hence there exists a domain $D' \subset D$ such that $a, a_1, b, b_1, c, c_1 \in D'$ and D' is the integral closure of the integers in a finite algebraic extension field of the rationals. Furthermore, D' is a Dedekind domain (see [31], Chapter 5, or [24] for details).

Therefore, by the proof of Proposition 2.1 in [6], p. 156, there exists $k \in D'$ such that $(a, b + kc) = D'$. Since $(a, b + kc) = D$ when the ideal is extended to D and since D is Bezout (see [24], pp. 85–86) it follows that D is an EDD.

EXAMPLE 2. The ring of entire functions is an EDD (see [21], p. 473, [18], and [19]).

DEFINITION. We shall say that n *is in the stable range of* R if R is a ring such that for $(a_1, \ldots, a_s, a_{s+1}) = R$ with $s \geqslant n$, there exist $b_1, \ldots, b_s \in R$ such that $(a_1 + b_1 a_{s+1}, a_2 + b_2 a_{s+1}, \ldots, a_s + b_s a_{s+1}) = R$ (see [13], pp. 344–345).

EXAMPLE 3. If D is a Bezout domain and has 1 in its stable range, then D is an EDD. In [13], p. 349, it is shown that if $a, b \in D$, then $(a, b) = (a + kb)$ for some $k \in D$. In addition if D is Bezout with 1 in its stable range and quotient field K and J is a domain such that $D \subset J \subset K$, then J has the same property [13], p. 350.

DEFINITION. A Kronecker function ring is defined as follows (see [13], p. 347 or [17], pp. 356–377): Suppose D is an integrally closed domain with quotient field K and suppose $\{R_v\}$ is the set of all valuation rings of K containing D and suppose v' is the *trivial extension* of v to $K(x)$ where x is an indeterminate over K, i.e., $v'(a_n x^n + \ldots + a_0) = \inf\{v(a_n), \ldots, v(a_0)\}$. If $R_{v'}$ is the valuation ring of v' and if $D' = \bigcap R_{v'}$, then D' is called the Kronecker function ring of D.

EXAMPLE 4. Kronecker function rings are EDD ([13], p. 347 or [17], p. 367).

DEFINITION. A domain D *has property* F if each nonzero element of D is contained in at most a finite number of maximal ideals.

If D is an F-domain, then $(a, b, c) = D$ implies $(a, b + kc) = D$ for some $k \in D$ ([6], p. 156). Hence a Bezout domain which is an F-domain must be an EDD; in particular a PID is an EDD.

EXAMPLE 5. A valuation ring is a domain in which the ideals are totally ordered under inclusion (see [32], [17], [3], and [25] for examples and properties of valuation rings). It is easy to see that a valuation ring is an EDD. In addition, if $V_1, \ldots, V_n$ are valuation rings with quotient field K, then it can be shown that $D = \bigcap_{i=1}^{n} V_i$ is an F-domain and a Bezout domain (see [17], p. 262 and [25], p. 38) and consequently D is an EDD.

EXAMPLE 6. The domains formed by Jaffard's "pullback theorem" ([20], [17]) are EDD. In fact, these domains have 1 in their stable range.

Suppose k is a field and G is a lattice ordered group. Let D' be the domain consisting of all formal sums $\{\sum_{i=0}^{n} a_i x^{\alpha_i} \mid a_i \in k, \alpha_i \in G\}$. Let K signify the quotient field of D'. Define $\varphi\colon D' \to G$ by $\varphi(\sum a_i x^{\alpha_i}) = \inf(\{\alpha_i\})_{i=1,\ldots,n}$. Extend φ to K by $\varphi(a/b) = \varphi(a) - \varphi(b)$ for $a/b \in K$. Then $D = \{X \in K \mid \varphi(X) \in G_+\}$ is a domain.

Suppose $X, Y \in D, X \neq 0, Y \neq 0$. We can assume $X = \sum a_i x^{\alpha_i}$, $Y = \sum b_i x^{\beta_i}$ since X and Y differ from these by a unit. Suppose $\varphi(X) = \lambda$ and $\varphi(Y) = \mu$. Since $\varphi(x^\lambda/X) = \varphi(X/x^\lambda) = 0$, we have x^λ/X and X/x^λ are

units of D. Since $(x^\lambda/X)\cdot X = x^\lambda$ and $(X/x^\lambda)\cdot x^\lambda = X$, it follows that $(x^\lambda) = (X)$. Likewise, $(x^\mu) = (Y)$.

If $\lambda = \mu$, then $(x^\lambda, x^\mu) = (x^\lambda) = (x^\mu)$. If $\lambda \neq \mu$, then $(x^\lambda, x^\mu) = (x^\lambda + x^\mu)$ since $x^\lambda/(x^\lambda + x^\mu)$ and $x^\mu/(x^\lambda + x^\mu) \in D$. If $(x^\lambda, x^\mu) = (x^\lambda + x^\mu)$, then $u_1 X = x^\lambda$, $u_2 Y = x^\mu$ for u_1, u_2 units of D which implies $(X, Y) = (u_1 X, u_2 Y) = (u_1 X + u_2 Y) = (X + (u_2/u_1) Y) = ((u_1/u_2) X + Y)$. If $(x^\lambda, x^\mu) = (x^\mu) = (x^\lambda)$, then $(X, Y) = (u_1 X, u_2 Y) = (u_2 Y) = (u_1 X)$. Either way 1 is in the stable range.

EXAMPLE 7. If B is a Bezout domain with quotient field K and M is the maximal ideal of the formal power series ring $K[[x]]$, then $B + M = D$ is a Bezout domain. Furthermore, if B has the property that $(a, b, c) = B$ implies $(ap, bp + cq) = B$ for some $p, q \in B$, then D has the same property.

If B is Bezout and if $M < A \subset D$ for A an ideal of D, then $A = A' + M$ where A' is an ideal of B and furthermore any set of generators of A' in B is a set of generators of A is D([17], pp. 560–561). If A is an ideal of D and $A \subset M$ and if $(a_1, a_2) = A$, then the following argument will show A is principal.

Suppose $a_1 = a_k x^k + a_{k+1} x^{k+1} + \ldots$ and $a_2 = b_l x^l + b_{l+1} x^{l+1} + \ldots$ with $a_k \neq 0$, $b_l \neq 0$, and $l \geqslant k \geqslant 1$. Since $a_1 = a_k x^k u_1$, $a_2 = b_l x^l u_2$ with u_1, u_2 units in D, then $(a_1, a_2) = (a_k x^k, b_l x^l)$. If $k < l$, then $(a_1, a_2) = (a_1)$. Suppose $k = l$. We can assume $a_k = a_k'/m$ and $b_l = b_k = b_k'/m$ with $a_k', b_k', m \in B$. Since B is Bezout, $(a_k', b_k') = (c)$. It follows easily that $(a_1, a_2) = (cx^k/m)$ and D is Bezout.

Suppose $(\alpha, \beta, \gamma) = D$ with $\alpha = a_0 + a_1 x + \ldots$, $\beta = b_0 + b_1 x + \ldots$, and $\gamma = c_0 + c_1 x + \ldots$ It is known that $k = k_0 + k_1 x + \ldots$ is a unit of D if and only if k_0 is a unit of B. ([25], p. 50 can be used to show this.) Hence $(a_0, b_0, c_0) = D$, so there exist $p_0, q_0 \in B \subset D$ such that $(a_0 p_0, b_0 p_0 + c_0 q_0) = B$. It follows easily that $(\alpha p_0, \beta p_0 + \gamma q_0) = D$. Hence D is an EDD if B is.

This example shows that an EDD of any finite dimension can be constructed, e.g., for an initial B take any PID (such as the integers).

A similar argument can be used to show that D has 1 in its stable range if B does. Furthermore, if $\{D_\alpha\}_{\alpha \in A}$ is a net of Bezout domains with 1 in the stable range, then $D' = \bigcup_{\alpha \in A} D_\alpha$ is a Bezout domain with 1 in the stable range as the following argument shows. In [13], p. 349, it is shown that a domain D is Bezout and has 1 in its stable range if and only if for any $a_1, a_2 \in D$ and $b \in (a_1, a_2)$, there exist $c, d \in D$ such that $b = c(a_1 + da_2)$. Suppose $a_1, a_2 \in D'$ and $b \in (a_1, a_2)$. Then $b = a_1 m + a_2 n$. There exists $\beta \in A$ such that $b, a_1, a_2, m, n \in D_\beta$ and hence $b \in (a_1, a_2)$ in D_β. Therefore, there exist $c, d \in D_\beta \subset D'$ such that $b = c(a_1 + da_2)$ in D_β and hence in D'.

EXAMPLE 8. Let K be an algebraically closed field of characteristic not 2. Let $x_1 = X$ be an indeterminate over K and suppose x_{n-1} is defined.

then x_n is defined by $x_{n-1} = x_n^2$. The set of $K[x_n, 1/x_n]$ forms a net and $\bigcup_{n=1}^{\infty} K[x_n, 1/x_n]$ is an EDD. This example is given in [4], p. 86. It is easily seen that $K[x_n]$ is a Euclidean domain and hence an EDD for n any natural number. Since $K[x_n] \subset K[x_n, 1/x_n] \subset K(x_n)$, then $K[x_n, 1/x_n]$ is an EDD by the remarks before Example 1 and $\bigcup K[x_n, 1/x_n]$ is an EDD.

5. Some additional results on Gaussian composition. In this section we consider the question of Gaussian composition for domains that may not be Bezout. The main result is Theorem 5.2 which gives a sufficient condition for the existence of a Gaussian compound of two forms with coprime divisors and the same discriminant. In addition we show that $D[x]$ is a G-domain when D is a PID (we wish to thank Professor Dennis R. Estes for suggestions in this connection), and we give a condition under which information concerning composition locally (i.e. in the quotient rings D_P, for P a prime ideal of D) yields global information (i.e. in D itself).

We recall that D is an F-domain provided every nonzero element of D is in at most finitely many maximal ideals of D. The following result is contained in Theorem 3.3 in [6], p. 162.

THEOREM 5.1. *If $f_i = [a_i, b_i, c_i]$ is a form of discriminant d and divisor Δ_i $(i = 1, 2)$ over an F-domain D such that $\Delta_1 + \Delta_2 = D$ and $b_1 - b_2 \in 2D$, then there exist united forms f_i' such that $f_i' \sim f_i$ for $i = 1, 2$.*

THEOREM 5.2. *Let D be a domain such that finitely generated projective D-modules are free (see [8] for definitions), and let $f = [a, b, c]$, $g = [a', b', c'] \in F(d)$ have divisors Δ, Δ' respectively. If $b - b' \in 2D$ and $\Delta + \Delta' = D$, then there exists a Gaussian compound of fg over D.*

Proof. Let M be a maximal ideal of D and consider the quotient ring D_M ([31], p. 219). Since $\Delta + \Delta' = D$, we have $\Delta D_M + \Delta' D_M = D_M$ and f, g have coprime divisors when considered as forms over D_M. Recalling the notation of Theorems 2.5 and 2.11, we associate with f, g the D-modules M_f, M_g respectively. It follows that $M_f D_M$, $M_g D_M$ are the D_M-modules associated with f, g respectively when considered as forms over D_M. Furthermore, $M_f M_g D_M = M_f D_M \cdot M_g D_M$. Noting that D_M is an F-domain, we see that there exists a direct compound of fg over D_M by Theorem 5.1, and as a consequence of Theorem 2.11, $M_f D_M \cdot M_g D_M$ is a free 2-dimensional D_M-module. We conclude that $M_f M_g D_M$ is a free 2-dimensional D_M-module for all maximal ideals M of D, which implies that $M_f M_g$ is a finitely generated projective D-module ([1], p. 141), hence a free D-module, and there exists a direct compound of fg by Theorem 2.11.

COROLLARY 5.3. *If D is a domain such that finitely generated projective D-modules are free and such that $x^2 \equiv y^2 \pmod 4$ implies $x \equiv y \pmod 2$ in D, then D is a G-domain.*

COROLLARY 5.4. *If D is a domain such that finitely generated projective D-modules are free and such that D_M is a G-domain for each maximal ideal M of D, then D is a G-domain.*

Proof. The corollary follows directly from Theorem 5.2 since $(x-y)/2 \in D_M$ for each maximal ideal M of D implies that $(x-y)/2 \in D$ ([25], p. 23).

COROLLARY 5.5. *If D is a* PID, *then the polynomial domain $D[x]$ is a G-domain.*

Proof. Applying Seshadri's theorem ([28], pp. 456–457), we have that finitely generated projective $D[x]$-modules are free when D is a PID. Furthermore, D is a PID implies that $D[x]$ is a unique factorization domain, and consequently $D[x]$ is integrally closed ([31], p. 261). By [6], p. 158, $D[x]$ has the property that $a^2 \equiv b^2 \pmod 4$ implies that $a \equiv b \pmod 2$, and the proof is completed by applying Theorem 5.2.

Remark. As we remarked earlier, an example is given in [6], p. 177, of a Noetherian, 2-dimensional (i.e. Krull dimension), unique factorization domain D which is not a G-domain. We note that D is integrally closed and therefore D_M is integrally closed for each maximal ideal M ([31], p. 261), so that D_M is a D-domain (and, therefore a G-domain) by Theorem 5.1. Thus it appears that we must have rather strong conditions holding in a domain in order to conclude that it is a G-domain (D-domain) due to the fact that it is locally a G-domain (D-domain).

Remark. We have shown that every D-domain is a G-domain, but the converse has not been settled. Out candidate for a counterexample (if one exists) is $Z[x]$, but we have been unable to show whether or not $Z[x]$ is a D-domain.

DEFINITION. Let D be a local domain of dimension 1 with maximal ideal m. Let $\bar{D}$ be the integral closure of D in K, the quotient field of D, and let $\bar{m}$ be the Jacobson radical of $\bar{D}$. Then D is said to be a *weak (discrete) valuation ring* if we have $m = \bar{m}$ in the set-theoretical sense.

DEFINITION. A Noetherian domain D is said to be a *weakly normal ring* provided

(a) For any prime ideal P of height 1 in D, D_P is a weak valuation ring.

(b) Any principal ideal ($\neq 0$) has the property that its prime divisors have height 1 in D.

The above definitions are from [12], p. 341, and [25] gives terms not defined above.

PROPOSITION 5.6. *If D is a semi-local, weakly normal ring of dimension 1, then $D[x, y]$, where x and y are indeterminantes over D, has the property that finitely generated projective modules are free. (In particular, if $D_{v_1}, \ldots, D_{v_n}$*

are rank 1, *discrete valuation rings with a common quotient field, then* $D = \bigcap_{i=1}^{n} D_{v_i}$ *satisfies the above hypothesis.*)

Proof. See [12], pp. 351–352.

COROLLARY 5.7. *If* D *is a semi-local, weakly normal ring of dimension* 1, *then* $D[x, y]$, *where* x *and* y *are indeterminates over* D, *has the property that a direct compound exists for any two forms with the same discriminant and coprime divisors whose middle coefficients are congruent* mod (2).

Proof. Easy, using Proposition 5.6 and Theorem 5.2.

COROLLARY 5.8. *If* D *is the intersection of a finite number of rank* 1, *discrete valuation rings having a common quotient field, then* $D[x, y]$ *is a G-domain where* x *and* y *are indeterminates. (In particular, if* $p_1, \ldots, p_n$ *are primes in* Z *and if* $Z_S = \bigcap_{i=1}^{n} Z_{(p_i)} (S = Z \setminus \bigcup_{i=1}^{n} (p_i))$ *then* $Z_S[x, y]$ *is a G-domain.*)

Proof. Immediate from Corollary 5.7 since D is a PID.

THEOREM 5.9. *If* D *is a domain, then a necessary and sufficient condition for* D *to be an F-domain is that* D_S *be an F-domain for every multiplicative system* S *of* D *containing a nonunit.*

Proof. It follows easily from the elementary properties of quotient rings that D_S is an F-domain when D is. ([31], pp. 218–233, provides a treatment of quotient rings.)

Suppose that D_S is an F-domain for each quotient ring D_S such that $D_S > D$. For each nonzero x in D denote by F_x the family of maximal ideals in D containing x and by F'_x the family of maximal ideals of D which do not contain x, and denote the Jacobson radical of D by $J(D)$.

If every nonunit of D is in $J(D)$, then $J(D)$ is the unique maximal ideal of D and D is an F-domain.

Let x be a nonunit of D such that $x \notin J(D)$. Then there is a maximal ideal M such that $x \notin M$, and hence there is an $m \in M$ such that $(x, m) = D$. If $S = \{m^n \mid n = 0, 1, 2, \ldots\}$, then $D_S > D$ and $M' D_S \neq D_S$ for $M' \in F_x$. Hence F_x is finite. Consequently, if $J(D) = (0)$, then D is an F-domain. Suppose $y \in J(D)$ with $y \neq 0$, and let $S' = \{x^n \mid n = 0, 1, 2, \ldots\}$. Now $D_{S'} > D$, $M'' D'_S \neq D_{S'}$ for $M'' \in F'_x$, $y \in M''$ for $M'' \in F'_x$, so that F'_x is finite. Thus if $J(D) \neq (0)$, there are only a finite number of maximal ideals in D, and D is an F-domain.

Remark. In the proof of the converse of Theorem 5.9, we only need to know that D_S is an F-domain for multiplicative systems S of the form $S = \{x^n \mid n = 0, 1, \ldots\}$ where $x \neq 0$ is a nonunit of D.

The following are some examples of F-domains: PID's, Dedekind domains, valuation rings, the intersection of a finite number of valuation rings with a common quotient field, $K[x, y]/(y^2 - f^2(x)g(x))$ where K is a field $(2 \neq 0)$ with f and g nonconstant polynomials in $K[x] \subset K[x, y]$ with g square free, any quasi-semi-local domain ([25]), any Noetherian domain that is one dimensional, any quotient overring of an F-domain (see above), Nagata's example of a Noetherian domain whose height is infinite ([25], p. 203), and the power series ring $D[[x]]$ where D is local or semi-local.

DEFINITION. If A is an ideal of a ring R, then let $J(A)$ denote the intersection of the maximal ideals containing A and let $J = \{\text{ideals } A \text{ of } R \mid J(A) = A\}$. A ring R is *J-Noetherian* provided the ideals of J satisfy the ascending chain condition (denoted acc). A prime ideal P in J which contains an ideal A of R is called a *J-component* of A if P is minimal among the primes of J containing A.

If R is J-Noetherian, then every ideal of R has only finitely many J-components. (See [13], p. 344, for details and references.)

PROPOSITION 5.10. *If* D *is a one-dimensional domain, then a necessary and sufficient condition for* D *to be J-Noetherian is that every nonzero ideal of* D *be contained in at most a finite number of maximal ideals.*

Proof. Suppose D is J-Noetherian. Then a nonzero ideal A is contained in only finitely many J-components and since D is 1-dimensional, the J-components of A are the maximal ideals containing A.

Suppose each nonzero ideal of D is contained in only a finite number of maximal ideals. Then $A \in J$ if and only if $A = (0)$ or A is a finite intersection of maximal ideals. Hence D is J-Noetherian.

COROLLARY 5.11. *If* D *is a* 1*-dimensional domain, then* D *is J-Noetherian if and only if* D *is an F-domain.*

Proof. If $A \in J$ and $A \neq (0)$, then there exists $0 \neq a \in A$ and a is contained in at most a finite number of maximal ideals and hence so is A. The converse is clear from Proposition 5.10.

Remark. The example in [6], p. 177, is 2-dimensional and J-Noetherian, but is not an F-domain.

In [9], p. 134–140, and [6], p. 160–167, one of the basic results used in creating united forms is that a primitive form represents primitively an element relatively prime to a given element. We state this result explicitly below and show the result is false for the domain $Z[x]$.

EXAMPLE. The domain $Z[x]$ does not have the following property. If $f = [a, b, c]$ is a form over D, E an ideal of D, $(a, b, c) \neq (0)$, $E \neq (0)$, and $(a, b, c) + E = D$, then there exists $r, s \in D$ such that $(ar^2 + brs + cs^2) + E = D$. (See [6], p. 157.)

Let $h = [7, 2x, 10(x^2+1)]$ be a form over D. The discriminant of h is $4(-69x^2 - 70)$. The form h is primitive since $-7 \cdot 7 + (-25x)2x +$

$+5(10\cdot(x^2+1)) = -49-50x^2+50x^2+50 = 1$. The polynomial $f(y) = y^2-(2x)y+70(x^2+1)$ in $(Z[x])[y]$ is irreducible by Eisenstein's criterian since $2\nmid 1$, $2\mid 2x$, $2\mid 70(x^2+1)$, $4\nmid 70(x^2+1)$ ([30], p. 250). There do not exist $c, d \in Z[x]$ such that $(7c^2+2xcd+10(x^2+1)d^2)+(x) = Z[x]$ by the following argument. Suppose there exist $c, d, e, f \in Z[x]$ such that $f[7c^2+2xcd+10(x^2+1)d^2]+ex = 1$ where $c = c_0+c_1x+\ldots+c_{n_c}x^{n_c}$, $d = d_0+d_1x+\ldots+d_{n_d}x^{n_d}$, etc. Then $f_0(7c_0^2+10d_0^2) = 1$ and hence $f_0 = 1$ and $7c_0^2+10d_0^2 = 1$ since $7c_0^2+10d_0^2 > 0$. We need only show that $7m^2+10n^2 \neq 1$ for $m, n \in Z$, but that is clear.

References

[1] N. Bourbaki, *Éléments de Mathématique, Algèbre Commutative*, Chaptres 1 et 2, Paris 1961.

[2] — *Éléments de Mathématique, Algèbre Commutative*, Chaptres 3 et 4, Paris 1961.

[3] — *Éléments de Mathématique, Algèbre Commutative*, Chaptres 5 et 6, Paris 1964.

[4] — *Éléments de Mathématique, Algèbre Commutative*, Chaptre 7, Paris 1965.

[5] H. S. Butts and B. J. Dulin, *Gaussian composition of binary quadratic forms*, submitted for publication.

[6] — and D. Estes, *Modules and binary quadratic forms over integral domains*, Linear Algebra and its Applications 1 (1968), pp. 153–180.

[7] — and Gordon Pall, *Modules and binary quadratic forms*, Acta Arith. 15 (1968), pp. 23–44.

[8] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton U., 1956.

[9] L. E. Dickson, *Introduction to the Theory of Numbers*, New York 1957.

[10] — *History of the Theory of Numbers*, Vol. 3, Washington 1923.

[11] Dirichlet–Dedekind, *Zahlentheorie*, ed. 2, Braunschweig 1871.

[12] S. Endo, *Projective modules over polynomial rings*, J. Math. Soc. Japan 15 (1963), pp. 339–352.

[13] D. Estes and J. Ohm, *Stable range in commutative rings*, J. Algebra 7 (1967), pp. 343–362.

[14] C. F. Gauss, *Disquisitiones Arithmetical*, New Haven 1966.

[15] L. Gillman and M. Henriksen, *Some results about elementary divisor rings*, Trans. Amer. Math. Soc. 82 (1956), pp. 362–365.

[16] — *Rings of continuous functions in which every finitely generated ideal is principal*, Trans. Amer. Math. Soc. 82 (1956), pp. 366–391.

[17] R. W. Gilmer, *Multiplicative Ideal Theory*, Ontario 1968.

[18] O. Helmer, *Divisibility properties of integral functions*, Duke Math. J. 6 (1940), pp. 345–356.

[19] — *The elementary divisor theorem for certain rings without chain condition*, Bull. Amer. Math. Soc. 49 (1943), pp. 225–236.

[20] P. Jaffard, *Contributions à l'étude des groupes ordonnés*, J. Math. Pures Appl. 32 (1953), pp. 203–280.

[21] I. Kaplansky, *Elementary divisors and modules*, Trans. Amer. Math. Soc. 66 (1949), pp. 464–491.

[22] — *Composition of binary quadratic forms*, Studia Math. 35 (1968), pp. 523–530.

[23] S. Lang, *Algebra*, Reading 1967.

[24] H. B. Mann, *Introduction to Algebraic Number Theory*, Columbus 1955.

[25] M. Nagata, *Local Rings*, New York 1962.

[26] G. Pall, *Composition of binary quadratic forms*, Bull. Amer. Math. Soc. 54 (1948), pp. 1171–1175.

[27] S. Saks and A. Zygmund, *Analytic Functions*, Warszawa 1965.

[28] C. S. Seshadri, *Triviality of vector bundles over the affine space K^2*, National Academy of Science 44 (1958), pp. 456–458.

[29] H. J. S. Smith, *Collected Mathematical Papers*, vol. 1, Bronx 1965.

[30] B. L. van der Waerden, *Modern Algebra*, New York 1953.

[31] O. Zariski and P. Samuel, *Commutative Algebra*, vol. 1, Princeton 1965.

[32] — — *Commutative Algebra*, vol. 2, Princeton 1960.

TEXAS A&M UNIVERSITY
College Station, Texas

LOUISIANA STATE UNIVERSITY
Baton Rouge, Louisiana

Received on 20. 7. 1970 (107)