PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 43, Number 2, April 1974

REPRESENTATIONS OF DECOMPOSABLE FORMS

CARTER WAID

ABSTRACT. Results connecting binary quadratic forms and their associated quadratic fields are extended to irreducible decomposable forms and their associated fields. A rational linear substitution that carries such a form into a nonzero rational multiple of itself is shown to correspond with a linear map which admits a unique decomposition as multiplication by a nonzero element of the field followed by an automorphism of the field. This correspondence is one-to-one whenever the form is nondegenerate.

1. **Introduction.** In recent papers by Butts and Pall [3], Butts and Estes [2], and Taussky [4], the representations of a rational multiple $c\psi$ of binary quadratic form ψ by another binary quadratic form ϕ are studied. In this paper we generalize these results to rational representations of powers of irreducible decomposable forms. We show (Corollary 3.1) that any irreducible decomposable form which does not properly represent zero (for decomposable forms this is equivalent to being nondegenerate) and whose degree is relatively prime to the number of its variables has only a finite number of rational automorphs. Another interesting result (Corollary 1.3) is that a norm preserving linear endomorphism of an algebraic number field (considered as a linear space over the rationals) which leaves the identity fixed is an automorphism of the field. This result is well known for quadratic fields and (in modified form) quaternion algebras, and provides one of the cornerstones for the theory of composition of binary and quaternary quadratic forms.

2. **Preliminaries.** Let L be a Galois extension of the rational number field Q with Galois group G. Let K be a subfield of L and $S \subseteq G$ a complete set of Q-isomorphisms[1] of K into L. $N(a)$ will always mean $N_{K/Q}(a)$.

Presented to the Society, January 22, 1971; received by the editors July 8, 1971 and, in revised form, November 22, 1972.

AMS (MOS) subject classifications (1970). Primary 10C10, 12A20; Secondary 12F10, 10M05.

Key words and phrases. Decomposable form, automorph, isometry similitude, norm form, field automorphism, Galois group.

[1] In general we will not distinguish notationally between an automorphism σ of L and its restriction to K.

For $\alpha=(a_1, \cdots, a_n) \in K^{n*}$ (i.e., $\alpha \neq 0$) and $X=(X_1, \cdots, X_n)$, where the X_i's are indeterminates, set $\alpha X=\sum a_i X_i$. The *norm form*

$$N(\alpha X) = \prod_{\sigma \in S} \sigma(\alpha X) \tag{2.1}$$

is a homogeneous decomposable polynomial with rational coefficients. It is simply the field norm of αX considered as a member of the extension $K(X_1, \cdots, X_n)$ over $Q(X_1, \cdots, X_n)$, and its degree d is the degree of the extension K/Q.

The following result is known [**1**, p. 80].

PROPOSITION. *If $a_1=1$ and $K=Q[a_1, \cdots, a_n]$, then the norm form $N(\alpha X)$ is irreducible. Conversely, every irreducible decomposable form is integrally equivalent to a constant multiple of such a norm form. If we let $Q\alpha$ denote the linear subspace $\sum Qa_i$ of K, it follows that $N(\alpha X)$ is irreducible if $1 \in Q\alpha$.*

Let a be a nonzero rational number and k a positive integer. Set

$$\phi(X) = a \cdot [N(\alpha X)]^k. \tag{2.2}$$

There are some obvious remarks one can make about the form ϕ. If $x=(x_1, \cdots, x_n) \in Q^n$ and $\sum a_i x_i=0$, then $\phi(x)=a[N(0)]^k=0$, and every representation of 0 by ϕ is obtained in such a manner. In fact, the collection of vectors x satisfying $\sum a_i x_i=0$ comprises the *radical* of ϕ. The radical is the subspace of all x such that $\phi(x+y)=\phi(y)$ for all y in Q^n. If the radical is 0 then ϕ is *nondegenerate*, otherwise, ϕ is *degenerate*. Thus ϕ is nondegenerate if and only if ϕ does not properly represent zero.

If $T=(t_{ij})$ is a rational (integral) $n \times m$ matrix and $Y_1, \cdots, Y_m$ are indeterminates, then the linear substitution $X=TY$ carries the form $\phi(X)$ into the form $\psi(Y)=\phi^T(Y)=\phi(TY)$. We say that ϕ *represents* ψ *rationally* (*integrally*) or that T is a rational (integral) *representation* of ψ by ϕ. Plainly ψ is also decomposable. In fact,

$$\psi(Y) = a[N(\alpha TY)]^k = a[N(\beta Y)]^k$$

where $\beta=\alpha T \in K^m$.

If c is a rational number, we say that T is a rational (integral) similitude of ϕ of scale c whenever $\phi^T=c\phi$.

3. **Main result.** We are now in a position to prove the principal result of this paper. O. Taussky [**4**] employed the technique used here to derive a similar result for binary quadratic forms.

Let a, b, c be rational numbers with $a, b \neq 0$, and let k be a positive integer. Let $\alpha=(a_1, \cdots, a_n) \in K^{n*}$, $\beta=(b_1, \cdots, b_m) \in K^{m*}$, and set

$$\phi(X) = a[N(\alpha X)]^k, \quad \text{and} \quad \psi(Y) = b[N(\beta Y)]^k. \tag{3.1}$$

THEOREM 1. *If $1 \in Q\beta$ and $K=Q[b_1, \cdots, b_m]$, and if T is a representation of $c\psi$ by ϕ, then there exists an automorphism μ of K and a unique number t in K such that*

(i) $t\mu(\beta)=\alpha T$, *and*

(ii) $(Nt)^k=bc/a$.

Moreover, if $c \neq 0$, μ is unique.

PROOF. We consider only the case $c \neq 0$, the situation being clear if $c=0$.

(i) On one hand

$$c\psi(Y) = bc\left[\prod_{\sigma \in S} \sigma\left(\sum b_i Y_i\right)\right]^k;$$

while on the other

$$\begin{aligned}\phi^T(Y) &= a\left[\prod_{\sigma \in S} \sigma\left(\sum a_i\left(\sum t_{ij} Y_j\right)\right)\right]^k \\ &= a\left[\prod_{\sigma \in S} \sigma\left(\sum\left(\sum a_i t_{ij}\right) Y_j\right)\right]^k.\end{aligned}$$

Since $\phi^T=c\psi$, and $L[Y_1, \cdots, Y_m]$ is a unique factorization domain, and since some σ in S is the identity on K, there is a unique $t \in L$, $t \neq 0$, and a $\mu \in S$ such that $t\mu(\sum b_j Y_j)=\sum (\sum a_i t_{ij}) Y_j$. Hence,

$$t\mu(b_j) = \sum a_i t_{ij} \qquad (j = 1, 2, \cdots, m). \tag{3.2}$$

Since $1 \in Q\beta$, we have $1 \in \mu(Q\beta)$, and it follows from (3.4) that $t \in Q\alpha \subseteq K$. Consequently, since $t \neq 0$, $\mu(b_j) \in K$ for every j, and since the b_j's generate K, μ determines a unique automorphism of K.

(ii) This follows by straightforward computation.

If U and V are linear subspaces of K or Z-modules in K, then the *residual quotient* $U:V$ is defined by

$$U:V = \{x \in K \mid xV \subseteq U\}.$$

The pair (t, μ) of the preceding theorem satisfies

$$t \in Q\alpha:\mu(Q\beta). \tag{3.3}$$

Conversely, any pair (t, μ) satisfying (3.3) and $(Nt)^k=bc/a$ gives rise to (possibly infinitely many) rational representations T of $c\psi$ by ϕ. If $S=(s_{ij})$ is an $n \times m$ rational matrix such that $\sum a_i s_{ij}=0$ for each j, then

$S+T$ is another representation of $c\psi$ by ϕ associated with the pair (t, μ), and all other representations associated with (t, μ) arise in this manner.

COROLLARY 1.1. *The collection of rational representations of $c\psi$ by ϕ, where the scale c is allowed to vary, is the union of a finite number of subspaces of the space of $n \times m$ rational matrices. There is one such subspace for each automorphism of K.*

COROLLARY 1.2. *If $\tau: K \to K$ is a linear map satisfying the identity $N(\tau x) = cNx$, where c is a nonzero rational, then there is a nonzero number t in K and an automorphism of μ of K such that $\tau(x) = t \cdot \mu(x)$.*

COROLLARY 1.3. *If σ is a linear endomorphism of K that preserves norms and satisfies $\sigma(1) = 1$, then σ is an automorphism of K.*

4. **Rational similitudes.** If a is a nonzero number in L, the map $x \to ax$ is a linear isomorphism on L and is denoted by a_L. Restrictions of a_L to linear subspaces of L will still be denoted by a_L.

Let U, V, and W denote linear subspaces of L. It is clear that $U:U$ is a subfield of L and that U is a vector space over $U:U$.

LEMMA. *Let* dim U = dim V. *If $x \in U:V$ and $x \neq 0$, then $x(W:U) = W:V$ and $x(V:W) = U:W$. Consequently, the subfields $U:U$ and $V:V$ are identical, and $U:V$ and $V:U$ are one-dimensional vector spaces over this subfield.*

PROOF. The map $x_L: V \to U$ is a monomorphism and since the dimensions agree, it is an isomorphism. Hence $xV = U$ and $V = x^{-1}U$. Since $x(W:U)V = (W:U)xV = (W:U)U \subseteq W$, and $x(V:W)W \subseteq XV = U$, it follows that $x(W:U) \subseteq W:V$ and $x(V:W) \subseteq U:W$.

In a similar fashion one can show that

$$x^{-1}(W:V) \subseteq W:U \quad \text{and} \quad x^{-1}(U:W) \subseteq V:W,$$

and equality follows.

We now assume that ϕ is given by (2.2), and that $1 \in Q\alpha$ and $K = Q[a_1, \cdots, a_n]$.

THEOREM 3. *Suppose that* dim $Q\alpha$ *and the degree d of $N(\alpha x)$ are relatively prime. Then for any rational number c there are only a finite number of rational similitudes of ϕ of scale c.*

PROOF. The degree d of ϕ is the degree of K/Q. $Q\alpha$ is a vector space of, say, dimension m over Q and of, say, dimension l over the subfield $Q\alpha:Q\alpha$. If h is the degree of the extension $(Q\alpha:Q\alpha)/Q$, then h divides d, and $m = hl$. Since d and m are coprime, we must have $h = 1$ and $Q\alpha:Q\alpha = Q$. For any automorphism μ the residual quotient $Q\alpha:\mu(Q\alpha)$ is either 0 or one-dimensional over Q. Consequently, there are at most two numbers t

in $Q\alpha:\mu(Q\alpha)$ such that $(Nt)^k=c$. Since there are only finitely many automorphisms μ of K, the theorem follows.

COROLLARY 3.1 *If $\phi(X_1, \cdots, X_n)$ is a nondegenerate decomposable form that is a power of an irreducible form ψ of degree d, and if d and n are relatively prime, then for any rational number c there are only a finite number of rational similitudes of ϕ of scale c.*

BIBLIOGRAPHY

1. Z. I. Borevič and I. R. Šafarevič, *Number theory*, "Nauka", Moscow, 1964; English transl., Pure and Appl. Math., vol. 20, Academic Press, New York, 1966, pp. 75–83. MR **30** #1080; **33** #4001.

2. H. Butts and D. Estes, *Modules and binary quadratic forms over integral domains*, Linear Algebra and Appl. **1** (1968), 153–180. MR **38** #4503.

3. H. Butts and G. Pall, *Modules and binary quadratic forms*, Acta Arith. **15** (1968), 23–44. MR **39** #6822.

4. O. Taussky, *Automorphs and generalized automorphs of quadratic forms treated as characteristic value relations*, Linear Algebra and Appl. **1** (1968), 349–356. MR **38** #2155.

DEPARTMENT OF MATHEMATICS, WEST CHESTER STATE COLLEGE, WEST CHESTER, PENNSYLVANIA 19380

Current address: Department of Mathematics, Drexel University, Philadelphia, Pennsylvania 19104