韓國數學教育學會誌<數學教育>
1984. 12, Vol. XXIII, No. 1

Journal of the Korea Society of Mathematical Education
Dec. 1984, Vol. XXIII, No. 1

A Theorem on the Composition of Quadratic Forms

by Kee-Soo Park
Korea University, Seoul, Korea

1. Introduction

Historically, the problem of composition of quadratic forms over a field F asks the following: for what value of m and n does there exist a formula

$$(X_1^2+\cdots+X_m^2)(Y_1^2+\cdots+Y_n^2)=Z_1^2+\cdots+Z_n^2 \qquad (*)$$

where $Z_1,\dots,Z_n$ are homogeneous bilinear forms in the two sets of variables $X_1,\dots,X_m, Y_1,\dots, Y_n$.

In (*) holds, then the Clifford algebra $C^{m-1,0}$ of the quadratic space $(m-1)\ \langle -1\rangle$ has an n-dimensional representation over the field F(**). Letting $\rho_F(n)$ denote the biggest possible value k such that $C^{k-1,0}$ has an n-dimensional representation over F, then the above says nothing more than $m\leqq\rho_F(n)$.

Radon proved that the converse of (**) also holds for $F=R$.

The conclusion of this paper shows the converse of (**) doesn't hold for $F=C$.

2. Preliminary and Main Results

Let (U,λ), (V,φ) be F-quadratic spaces, of dimension m and n. If there exists a bilinear pairing $U\times V\to V$ denoted by $(x,y)\mapsto x\cdot y$, such that $\varphi(x,y)=\lambda(x)\cdot\varphi(y)$ for all $x\in U$, $y\in V$ (***), (***) reduces to (*) in the special case where $\lambda\cong m\langle 1\rangle$, $\varphi\cong n\langle 1\rangle$. For a vector $u\in U$, with $\lambda(u)\neq 0$, we can make $\lambda(u)=1$, and u acts as the identity on V by multiplication on scaling λ by a multiple and modifying the multiplication.

The following theorem by Radon gives idea to prove our main theorem.

Theorem (Radon). *The formula* (*) *exists for the field* $F=R$ *iff* $m\leqq\rho_R(n)$

Proof. The "only if" part holds for an arbitary field F, and is found in [1].

We prove here only the "if" part.

Assume $m\leqq\rho_R(n)$. Let $\{e_1,\dots,e_m\}$ be an orthonormal basis for (U,λ) and $U_0=\sum_{i\geq 2} Fe_i$. Then the Clifford algebra of $(U_0,-\lambda)$ becomes $C=C(U_0,-\lambda)=C^{m-1,0}$. Since $\varphi\cong n\langle 1\rangle$, we may think of the quadratic space (V,B,φ) as R^n equipped with the usual inner product. By definition of ρ_R, there exists a linear representation $L: C\to \mathrm{End}\,V=M_n(R)$. Let G be the multiplicative group, generated by the invertible elements $e_i (2\leqq i\leqq m)$ and -1 in C.

Since we have the relations $e_i^2=-1$, $e_ie_j=-1$, $e_ie_j=-e_je_i$ for $2\leqq i\neq j\leqq m$, G is obviously a finite group.

By the theory of group representation $L: C\to M_n(R)$ is equivalent to an orthogonal representation. Thus, after changing L by a conjugation on $M_n(R)$, we may assume that each $L(e_i)$ $(2\leqq i\leqq m)$ is an isometry on R^n. The rule $(x,y)\mapsto x\cdot y=L(x)(y)$ clearly defines a bilinear pairing $U_0\times V\to V$, and it satisfies

$$B(y,\ e_iy)=B(e_iy,\ e_i(e_iy))=-B(e_iy,y)\quad(2\leq i\leq m,\ y\in V).$$

This shows $B(y,e_iy)=0$, and hence $B(y,x\cdot y)=0$ for $x\in U_0$, $y\in V$.

We may now create a pairing $U\times V\to V$, by $(\alpha u+x)\cdot y=\alpha y+L(x)(y)$ $(\alpha\in F,\ x\in U_0, y\in V)$. This is easily checked to be bilinear. Then it is clear $B(y,\ L(x)(z))+B(z,L(x)(y))=0$ $(y,z\in V,\ x\in U_0)$. Replacing z by $L(x)(z)$, and using $L(x)^2=-\lambda(x)\cdot 1_v$, we obtain $\lambda(x)\ B(y,z)=B(x\cdot y,x\cdot z)$ whenever $x\in U_0$. A simple calculation shows that the same holds for any $x\in U$(assuming, of course, $\lambda(u)=1$). Putting $y=z$, we capture (**), and thus we obtain (*).

With a classical result of Schur in group representation theory [3], we can prove our main theorem.

Main Theorem. *If (*) holds over the complex field C, then it already exists for the real field R.*

Proof. Keeping all notations in the preceding proof.

Thus U, V denote R^m, R^n, C denotes the real Clifford algebra $C^{m-1,0}$, etc. We write "bar" to denote complexification $C\otimes R$.⁻

Assume (*) exists over C. Then we get a representation $\sigma:\bar{C}\longrightarrow \mathrm{End}_C\bar{V}$.

Since $\bar{B}(e_iy,\ e_iz)=\bar{\lambda}(e_i)\bar{B}(y,z)=\bar{B}(y,z)$ for $y,z\in\bar{V}$, restricted to G is a representation of G by complex orthogonal matrices. By the theorem of Schur, $\sigma|_G$ is equivalent to a real representation, and hence equivalent to a suitable real orthogonal representation. Changing σ by conjugation if necessary, we may suppose that $\sigma(G)\subset O(V,\varphi)$, here $O(V,\varphi)$ denotes the group of isometries of V. Since G spans C as a real algebra, we conclude $\sigma(C)\subset\mathrm{End}_R(V)$. By Radon's theorem we conclude that the formula (*) exists for R.

As an application we prove that the converse of(**) doesn't hold for $F=C$.

Corollary. *The converse of (**) doesn't hold for F=C.*

Proof. Let n be such that $\rho_R(n)<\rho_C(n)=m$. Then the complex Clifford algebra $C^{m-1,0}$ has an n-dimensional C-representation. If the converse of (**) hold, our theorem induce a contradiction.

References

1. T.Y. Lam, *The algebraic theory of quadratic forms*, Bejamin, 1973.
2. O.T. O'Meara, *Introduction to quadratic forms*, Springer-Verlag, 1963.
3. I. Reiner, *Linear representation of finite groups and associative algebras*, Interscience, 1962.