

FINITE ROTATION GROUPS IN LOW DIMENSIONS

DONALD K. FRIESEN

1. Introduction. Let V be a vector space of dimension two, three, or four over a field of characteristic not two, and let V have a non-singular orthogonal metric. The problem discussed in this paper is the determination of all finite groups that can occur as subgroups of the rotation group of V .

It is easily shown that for dimension two, all such groups are cyclic. Then by constructing a permutation representation for a three-dimensional group, we show that these groups are the ones that can occur in Euclidean 3-space, projective linear groups, and certain solvable groups described at the beginning of §3. Using results from (1), we then prove that in dimension four all finite groups, modulo a possible two-element subgroup of the centre, are sub-direct products of the three-dimensional ones.

2. Preliminaries and the anisotropic case. Throughout the paper, k will denote a commutative field of characteristic different from two. V will be a non-singular orthogonal geometry over k , $O(V)$ will be the group of isometries, and $O^+(V)$ the group of rotations.

The first objective is to show that we can assume that k is algebraically closed without a fear of losing some finite subgroups of $O^+(V)$. Suppose k is a subfield of K . Then $W = V \otimes_k K$ can be made into a non-singular geometry over K in a natural way so that the usual embedding of V into W is k -linear and preserves the inner product. Each isometry of V extends to an isometry of W , thereby inducing a monomorphism of $O(V)$ into $O(W)$ and by restriction of $O^+(V)$ into $O^+(W)$. Hence a finite subgroup of $O^+(V)$ is isomorphic to a subgroup of $O^+(W)$. Thus by passing from k to its algebraic closure, we may pick up additional finite subgroups, but we shall not lose any. From now on we adopt the simplification that k is algebraically closed.

PROPOSITION 2.1. *If V has dimension two, then all finite subgroups of $O^+(V)$ are cyclic.*

Proof. The proposition follows immediately from two well-known results: first that the only two-dimensional orthogonal geometry over an algebraically closed field is hyperbolic, and second that the rotation group of a hyperbolic plane

Received October 17, 1966. This work was partially supported by a grant from the Carnegie Foundation. It is based on the author's doctoral dissertation at Dartmouth College written under the direction of Professor Ernst Snapper.

is isomorphic to the multiplicative group of the field. Since finite subgroups of the multiplicative group of k are cyclic, we complete the proof.

Next we shall constrict a permutation representation for a subgroup G of $O^+(V)$ when V has dimension three. We distinguish two cases. Let $A(\sigma)$ denote the axis of σ for $\sigma \neq 1$ in G .

Case 1. $A(\sigma)$ is anisotropic for all such σ .

Since k is algebraically closed, $A(\sigma)$ contains two vectors whose length is 1. The set, X , of all such vectors for all non-identity rotations in G is the set G will act on. The action of G on X is the obvious one: every rotation of G carries a vector of X into another such vector.

Case 2. There exists $\sigma \in G$, $\sigma \neq 1$, such that $A(\sigma)$ is isotropic.

In this case we add to the set X the set Y of all isotropic lines which are left invariant by some non-identity element of G . They need not be left pointwise invariant. Then G acts on $Z = X \cup Y$.

The two cases yield very different results and will be treated separately. The proof for Theorem 1, which provides the solution to Case 1, is the same proof given in (2, pp. 270–275) when k is the field of real numbers and will be sketched in this section. Case 2 is much more complicated, and the remainder of the paper is essentially devoted to it.

THEOREM 1. *If G is a finite subgroup of a three-dimensional rotation group, and if the axis of each non-identity rotation is anisotropic, then G is isomorphic to one of the finite groups of rotations of a Euclidean 3-space:*

- (1) *a cyclic group,*
- (2) *a dihedral group,*
- (3) *the tetrahedral group,*
- (4) *the octahedral group,*
- (5) *the icosahedral group.*

The proof of Theorem 1 depends on a close examination of the permutation representation (G, X) . Since we shall need the same sort of results in Case 2, we state everything in terms of (G, Z) . Clearly, any domain of transitivity of Z lies wholly within X or Y ; therefore, let

$$X = X_1 \cup \dots \cup X_n,$$

$$Y = Y_1 \cup \dots \cup Y_m$$

be a decomposition into domains of transitivity, and let $x_i = |X_i|$, $y_i = |Y_i|$, where $| \cdot |$ denotes cardinality. Writing $H(P)$ for the group of elements of G leaving $P \in Z$ fixed, we have $|H(P)| = |G|/x_i$, where $P \in X_i$. We let $g = |G|$ and $\bar{x}_i = g/x_i$, $\bar{y}_i = g/y_i$.

Let $F = \{(\sigma, z) \mid \sigma \in G, z \in Z, \sigma z = z\}$. The number of “fixed pairs” in F can be obtained by first letting σ vary through G and then allowing z to vary through Z , obtaining

$$|F| = \sum_{i=1}^n x_i(\bar{x}_i - 1) + \sum_{i=1}^m y_i(\bar{y}_i - 1),$$

or by doing the reverse, obtaining

$$|F| = 4g_1 + g_2,$$

where g_1 is the number of elements of G with anisotropic axes and g_2 the number with isotropic axes. Thus we have

PROPOSITION 2.2.

$$(a) \quad 4g_1 + g_2 = \sum_{i=1}^n x_i(\bar{x}_i - 1) + \sum_{i=1}^m y_i(\bar{y}_i - 1),$$

$$(b) \quad 2g_1 = \sum_{i=1}^n x_i(\bar{x}_i - 1).$$

COROLLARY 2.3. $n \leq 3$.

Proof. Since $g_1 \leq g - 1$ we have

$$2\left(1 - \frac{1}{g}\right) \geq \sum_{i=1}^n x_i(\bar{x}_i - 1)/g = \sum_{i=1}^n (1 - 1/\bar{x}_i) \geq n(1/2).$$

In the case where all axes are anisotropic the first inequality becomes equality, and the proof given in (2, pp. 270–275) carries over almost word for word using Proposition 2.1 to show that $H(P)$ is cyclic for each $P \in X$. This gives us Theorem 1.

3. The isotropic case. If G contains a rotation with isotropic axis, the main result is

THEOREM 2. *If G is a finite subgroup of a three-dimensional rotation group, and if G contains a non-identity rotation with an isotropic axis, then G is isomorphic to one of the following:*

- (1) *the additive group of a finite-dimensional vector space over $\text{GF}(p)$, where p is an odd prime,*
- (2) *a Frobenius group with regular subgroup as in (1) and with cyclic quotient,*
- (3) *a projective special linear group over a finite field,*
- (4) *a projective general linear group over a finite field.*

The proof is carried out in a manner analogous to that in the anisotropic case. We shall use the permutation representation to obtain information about the order of G and show that unless every element of G leaves some point of Z fixed, with few exceptions, G is not solvable. Then using the fact that G has a non-trivial partition, a theorem of Suzuki tells us precisely what groups can occur.

We begin by investigating the structure of $H(P)$ for P in Y . Let N be a vector on P . Then $\sigma \in H(P)$ implies that $\sigma N = aN$, $a \in k^*$, the multiplicative group of non-zero elements of k . The map which sends σ onto a is a homomorphism from $H(P)$ into k^* with kernel $K = \{\sigma \mid \sigma \in G \text{ and } A(\sigma) = P\} \cup \{1\}$. K is then isomorphic to a subgroup of the additive group of k (1, p. 133). Hence the characteristic of k is $p \neq 0$, and K is as described in (1) of Theorem 2. Since $H(P)/K$ is isomorphic to a subgroup of k^* , it must be cyclic.

LEMMA 3.1. *If p is the characteristic of k , then $\sigma^p = 1$ if and only if $A(\sigma)$ is isotropic or $\sigma = 1$.*

Proof. Obviously, if $A(\sigma)$ is isotropic or if $\sigma = 1$, then $\sigma^p = 1$. Conversely, if $A(\sigma)$ is anisotropic, then the group of rotations with $A(\sigma)$ as axis is isomorphic to a subgroup of k^* , which can contain no elements of order p . Note that this does not depend on $\sigma \in H(P)$.

PROPOSITION 3.2. *$H(P)$ is a Frobenius group (unless $H(P) = K$).*

Proof. Let $\sigma \in H(P)$. Then by the lemma, the order of σ is p or it divides the order of $H(P)/K$. Hence by (3, p. 587), $H(P)$ is a Frobenius group.

COROLLARY 3.3. *$[H(P):K] \mid (p^r - 1)$, where p^r is the order of K .*

COROLLARY 3.4. *$H(P)$ contains a cyclic subgroup of order $[H(P):K]$ and all such groups are conjugate in $H(P)$. Moreover, $[H(P):K] = \bar{x}_i$ for some i .*

Proof. $H(P)$ is the semidirect product of K and $H(P)/K$, since they have relatively prime orders. The second claim follows from Sylow theory for solvable groups. Finally, $H(P)/K$ is cyclic so that $H(P)/K$ is isomorphic to $H(Q)$ for some Q in the orthogonal complement of P .

Now let us go back to the more general group G . We assume that G has at least one rotation with an isotropic axis.

PROPOSITION 3.5. *Suppose every non-identity rotation in G has an isotropic axis. Then $G = H(P)$, i.e., all rotations have the same axis.*

Proof. By Proposition 2.2,

$$g_2 = \sum_{i=1}^m y_i(\bar{y}_i - 1).$$

Hence

$$1 > \frac{g_2}{g} = \sum_{i=1}^m (1 - 1/\bar{y}_i) \geq m \cdot (1/2)$$

which implies $m = 1$. But

$$g - 1 = g_2 = y_1(\bar{y}_1 - 1) = g - y_1,$$

and we have $y_1 = 1$.

PROPOSITION 3.6. *If $p|\bar{y}_i$ and $p|\bar{y}_j$, then $i = j$.*

Proof. If H is a p -Sylow subgroup of G , then by the preceding proposition, $H = H(P)$ for some $P \in Y$. All such subgroups are conjugate; hence all $Q \in Y$ which are axes of rotations in G are conjugate. If $p|\bar{y}_i$, then Y_i consists of these axes. Thus $i = j$.

PROPOSITION 3.7. $g_2 = y_i(p^r - 1)$, where p^r is the order of the p -Sylow subgroup and $p|\bar{y}_i$.

Proof. Let N be a vector on $Q \in Y_i$ and $K = \{\sigma \mid \sigma \in G \text{ and } \sigma N = N\}$. Then $\psi K \psi^{-1} = K$ if and only if $\psi \in H(Q)$, since $A(\psi \sigma \psi^{-1}) = \psi A(\sigma)$. Hence $H(Q)$ is the normalizer of K , and the number of subgroups of order p^r is y_i . Since they are obviously disjoint, the proposition is proved.

Our next project is to determine the possible values n and m may have.

PROPOSITION 3.8. $n \leq 2$.

Proof. By Corollary 2.3 we know that $n \leq 3$. We assume, therefore, that $n = 3$ and derive a contradiction. Assume the ordering such that

$$\bar{x}_1 \leq \bar{x}_2 \leq \bar{x}_3.$$

Then if $\bar{x}_1 \geq 3$, we have

$$1 - 1/\bar{x}_1 + 1 - 1/\bar{x}_2 + 1 - 1/\bar{x}_3 \geq 2,$$

whereas $g_1/g < 1$. These two inequalities are incompatible, as are similar ones if $\bar{x}_1 = 2, \bar{x}_2 \geq 4$, or $\bar{x}_1 = 2, \bar{x}_2 = 3, \bar{x}_3 \geq 6$.

If $\bar{x}_1 = 2, \bar{x}_2 = 3, \bar{x}_3 = 3, 4$, or 5 , then

$$g_1/g \geq 1/2(1 - 1/2 + 1 - 1/3 + 1 - 1/3) \geq 11/12.$$

By Proposition 3.7,

$$g_2 = y_i(p^r - 1)$$

where $p^r|\bar{y}_i$.

$$g_2/g = (p^r - 1)/\bar{y}_i = (1 - 1/p^r)/\bar{x}_i \geq (2/3)(1/5);$$

therefore $(g_1 + g_2)/g > 1$, which is impossible. The only remaining alternative is that $\bar{x}_1 = \bar{x}_2 = 2$. In this case

$$g_1/g = 1 - 1/2\bar{x}_3,$$

$$g_2/g = (1 - 1/p^r)/\bar{x}_i \geq 2/3\bar{x}_3.$$

Again $(g_1 + g_2)/g > 1$.

PROPOSITION 3.9. *If $n = 1$, then G is isomorphic to A_4 .*

Proof. Suppose $n = 1$. Then $\bar{x}_1|\bar{y}_i$ for some i , say $i = 1$. By Proposition 2.2,

$$g_1 + g_2 = \sum_{i=1}^m y_i(\bar{y}_i - 1) - x_1(\bar{x}_1 - 1)/2.$$

Hence

$$1 > 1 - \frac{1}{g} = \sum_{i=2}^m (1 - 1/\bar{y}_i) + 1 - 1/\bar{y}_1 - (1 - 1/\bar{x}_1)/2.$$

Since $\bar{x}_1 \leq \bar{y}_1$,

$$1 - 1/\bar{y}_1 - (1 - 1/\bar{x}_1)/2 \geq (1 - 1/\bar{y}_1)/2$$

and thus

$$1 > \sum_{i=2}^m (1 - 1/\bar{y}_i) + (1 - 1/\bar{y}_1)/2.$$

Note that m cannot be 1 since then

$$1 - 1/g = 1 - 1/\bar{y}_1 - (1 - 1/\bar{x}_1)/2 < 1/2,$$

which is impossible.

Each $\bar{y}_i \geq 2$, at least one $\bar{y}_i \geq 3$, and if this is \bar{y}_1 , it must be at least 6 since $p|\bar{y}_i$ and $\bar{x}_1|\bar{y}_i$ with $(p, \bar{x}_1) = 1$. Hence m cannot be 3, or greater, and thus $m = 2$. Also we must have $\bar{y}_1 = 2 = \bar{x}_1$ and $\bar{y}_2 = 3$. Then $1 - 1/g = 11/12$ and $g = 12$. Since $\bar{y}_2 = 3$, $y_2 = 4$ and G is a subgroup of the group S_4 of all permutations of Y_2 . Hence G must be isomorphic to A_4 .

We have now shown that $n = 2$ except in certain special cases which are easily handled.

PROPOSITION 3.10. *If $n = 2$, then $m = 2$.*

Proof. We are assuming throughout that $m \neq 0$. Suppose $m = 1$. Then

$$g_2/g = 1 - 1/\bar{y}_1 - (1 - 1/\bar{x}_1) - (1 - 1/\bar{x}_2).$$

Now $\bar{y}_1 = \bar{x}_1 p^r$ for some r , $(\bar{x}_1, p) = 1$, and $\bar{y}_1 = \bar{x}_2 p^r$ for some r ,

$$(\bar{x}_2, p) = 1.$$

Hence $\bar{x}_1 = \bar{x}_2$, $\bar{y}_1 = \bar{x}_1 p^r$.

$$g_2/g = 1 - 1/(\bar{x}_1 p^r) - 2/(1 - 1/\bar{x}_1).$$

But $2(1 - 1/\bar{x}_1) \geq 1$, therefore $g_2/g < 0$, which is impossible.

Thus we have $m \geq 2$. If $m \geq 3$, we can suppose the x_i, y_i are numbered so that $\bar{y}_1 = \bar{x}_1$, $\bar{y}_2 = \bar{x}_2$ or \bar{x}_1 , and $p|\bar{y}_3$. For if $p|\bar{y}_3$, \bar{y}_1 and \bar{y}_2 are prime to p and hence must equal \bar{x}_1 or \bar{x}_2 .

In the first case

$$g_2 = y_3(p^r - 1)$$

by Proposition 3.7, and

$$g_2 = \sum_{i=1}^m y_i(\bar{y}_i - 1) - \sum_{i=1}^2 x_i(\bar{x}_i - 1) \geq y_3(\bar{y}_3 - 1).$$

Thus $g_2/g \geq 2/3$, whereas $g_1/g \geq 1/2$ making $g_1 + g_2 > g$. Suppose we have the second situation. We may assume that $\bar{x}_2|\bar{y}_3$, since \bar{x}_1 cannot, and if $\bar{y}_3 = p^r$, then $g_2 \geq 2g/3$. Then

$$g_2 \geq x_1(\bar{x}_1 - 1) + x_1(\bar{x}_1 - 1) + y_3(\bar{y}_3 - 1) - x_1(\bar{x}_1 - 1) - x_2(\bar{x}_2 - 1),$$

$$g_2/g \geq 1 - 1/\bar{x}_1 \geq 1/2,$$

since $\bar{x}_2 < \bar{y}_3$. Again $g_1 + g_2 > g$.

We now know that, unless G is A_4 or the additive group of a vector space, $n = m = 2$. We now show that unless $G = H(P)$ for some P in Y , then G is as described in (3) or (4) of Theorem 2. The first step is to determine the order of G .

PROPOSITION 3.11. *If $n = m = 2$ and if $G \neq H(P)$ for any P in Y , then the order of G is $p^r(p^r + 1)(p^r - 1)$ or $p^r(p^r + 1)(p^r - 1)/2$ unless $p = 3$, and then G may also be A_5 .*

Proof. We assume that the domains of transitivity are numbered so that $\bar{x}_1 = \bar{y}_1$, $p^r\bar{x}_2 = \bar{y}_2$, where p^r is the order of the p -Sylow subgroup of G . From Proposition 2.2 we deduce that

$$g_2 = x_2 - y_2,$$

$$2g_1 = x_1(\bar{x}_1 - 1) + x_2(\bar{x}_2 - 1) = 2g - x_1 - x_2.$$

Thus

$$g - 1 = g + (x_2 - x_1)/2 - y_2,$$

from which it follows that

$$(3.1) \quad x_2 - x_1 = 2(y_2 - 1),$$

and dividing by g

$$(\bar{x}_1 - \bar{x}_2)/\bar{x}_1 \bar{x}_2 = 2(y_2 - 1)/g.$$

Since $g = x_2 \bar{x}_2 = y_2 p^r \bar{x}_2$,

$$(3.2) \quad y_2 p^r (\bar{x}_1 - \bar{x}_2) = 2\bar{x}_1(y_2 - 1).$$

Hence $p^r|(y_2 - 1)$, i.e., $y_2 = 1 + cp^r$.

We know that $c \geq 1$ since $G \neq H(P)$ for any P . We shall prove that $c = 1$, except in the one special case mentioned in the proposition. From (3.2) we also see that $y_2|2\bar{x}_1$. Now $\bar{x}_1 \leq y_2$ since for $P \in Y_2$, $\sigma, \sigma' \in H(Q)$ for some $Q \in X_1$ implies that $\sigma P \neq \sigma' P$. Hence either (Case 1) $y_2 = \bar{x}_1$, or (Case 2) $y_2 = 2\bar{x}_1$. In both cases, since $y_2|x_2$, we have $\bar{x}_1|x_2$. Also $\bar{x}_2|\bar{y}_2$ and $\bar{y}_2|x_1$, therefore $\bar{x}_2|x_1$. Rewriting (3.1) we obtain

$$x_1 - 2 = y_2(p^r - 2).$$

Therefore $(x_1, y_2) \leq 2$. Using the facts that $\bar{x}_1|y_2$ and $\bar{x}_2|x_1$, we obtain

$$(\bar{x}_1, \bar{x}_2) \leq 2.$$

Case 1. Suppose $\bar{y}_2 = x_1$. Then from (3.1) we have $y_2 - \bar{x}_2 = 2c$. Thus

$$(3.3) \quad \bar{x}_2 = 1 - 2c + cp^r.$$

Applying Corollary 3.3,

$$1 - 2c + cp^r \leq p^r - 1$$

and hence

$$c(p^r - 2) \leq p^r - 2.$$

We conclude that $c = 1$ if $x_1 = \bar{y}_2$.

Case 2. Suppose that $y_2 = 2\bar{x}_1 = 1 + cp^r$. Then clearly c must be odd. Again from (3.1), $y_2 - 2\bar{x}_2 = 2c$. Thus

$$(3.4) \quad 2\bar{x}_2 = 1 - 2c + cp^r.$$

By Corollary 3.3,

$$1 - 2c + cp^r \leq 2(p^r - 1),$$

$$c(p^r - 2) \leq 2(p^r - 2) + 1.$$

Therefore $c < 3$ unless $p^r - 2 = 1$, and then c might be 3. Temporarily ignoring this possibility we see that $c = 1$. Now from (3.3) we observe that if $y_2 = \bar{x}_1$, then $\bar{x}_2 = p^r - 1$ and

$$g = (p^r + 1)p^r(p^r - 1),$$

and if $2\bar{x}_1 = y_2$, from (3.4), we have that

$$g = p^r(p^r + 1)(p^r - 1)/2.$$

Returning to the special case $p^r = 3$, we observe that by (3.4) we have $\bar{x}_2 = 4$ and $g = 60$. Since G acting on $Y_2 \cup X_1 \cup X_2$ satisfies the same properties that determine A_5 in the anisotropic case, the proof given in (2, pp. 270–275) shows that G is indeed A_5 .

PROPOSITION 3.12. *If $G \neq H(P)$ for any P in Y , and if $g \geq 60$, then G is not solvable.*

Proof. Suppose G' is a normal subgroup of G , where

$$g = p^r(p^r + 1)(p^r - 1)/2,$$

and that there is a rotation in G' with isotropic axis. Then G' must contain rotations with each element of Y_2 as axis since G acts transitively on Y_2 . The only groups which have $y_2 = p^r + 1$ are those of order greater than or equal to that of G if $p^r > 3$. Hence $G = G'$ and G is in fact simple.

Suppose now that G' contains no rotation with isotropic axis. Let $\sigma \in G'$, $\sigma \neq 1$. Then $A(\sigma) \in X_i$ and G' must contain rotations with axis P for all $P \in X_i$. Since $p|x_i$, G' must contain rotations of order p , contradicting Lemma 3.1.

The same argument shows that if G has order $p^r(p^r + 1)(p^r - 1)$, the only normal subgroup it can have is of index 2. Since A_5 is also non-solvable, the proposition is proved.

Remark. The only cases excluded by the restriction $g \geq 60$ are $g = 24$ and $g = 12$. In these cases it is easy to describe G as a subgroup of S_4 ; hence G would be S_4 or A_4 .

We say that a group G has a non-trivial partition if there is a collection of proper subgroups $\{G_i, i = 1, \dots, s\}$ such that $G_i \cap G_j = \{1\}$ if $i \neq j$ and $G_1 \cup \dots \cup G_s = G$. A three-dimensional rotation group has an obvious partition indexed by the axes of elements of G :

$$G_A = \{\sigma \mid \sigma \in G \text{ and } A(\sigma) = A \text{ or } \sigma = 1\}.$$

Now we apply a result of Suzuki (4, p. 241), in which it is stated that a non-solvable group with a non-trivial partition is either $\text{PSL}(2, p^r)$, $\text{PGL}(2, p^r)$, or one of a collection of simple groups whose orders are not divisible by 3. Observing that $p^r(p^r + 1)(p^r - 1)$ is divisible by 3, we see that the non-solvable groups are projective groups. Thus we have completed the proof of Theorem 2.

Note that the cases where G is isomorphic to A_5 , S_4 , or A_4 are covered since $\text{PSL}(2, 5)$ is isomorphic to A_5 , $\text{PGL}(2, 3)$ to S_4 , and $\text{PSL}(2, 3)$ to A_4 .

We conclude the paper with some remarks about rotation groups in four-dimensional spaces. Again assuming k is algebraically closed, we apply a result from (1, p. 203) to show that the commutator subgroup of $O^+(V)$ modulo its centre is isomorphic to $\text{PSL}(2, k) \times \text{PSL}(2, k)$. However, with k algebraically closed, $O^+(V)$ is its own commutator subgroup. Since the centre of $O^+(V)$ is $\{\pm 1_V\}$ and $\text{PSL}(2, k)$ is the three-dimensional rotation group for a non-singular subspace of V , we conclude that, modulo a possible two-element subgroup of the centre, every finite subgroup of $O^+(V)$ is a subdirect product of two three-dimensional groups.

REFERENCES

1. E. Artin, *Geometric algebra* (Interscience, New York, 1957).
2. H. S. M. Coxeter, *Introduction to geometry* (Wiley, New York, 1961).
3. W. Feit, *On the structure of Frobenius groups*, Can. J. Math., 9 (1957), 587–596.
4. M. Suzuki, *On a finite group with a partition*, Arch. Math., 12 (1961), 241–254.

*University of Illinois,
Urbana, Illinois*