ANTICOMMUTING LINEAR TRANSFORMATIONS

H. KESTELMAN

1. It is well known that any set of four anticommuting involutions (see § 2) in a four-dimensional vector space can be represented by the Dirac matrices

$$(1) \quad B_{2,0} = \begin{pmatrix} 1_2 & 0 \\ 0 & -1_2 \end{pmatrix}, B_{2,1} = \begin{pmatrix} 0 & B_{1,0} \\ B_{1,0} & 0 \end{pmatrix}, B_{2,2} = \begin{pmatrix} 0 & B_{1,1} \\ B_{1,1} & 0 \end{pmatrix}, B_{2,3} = \begin{pmatrix} 0 & B_{1,2} \\ B_{1,2} & 0 \end{pmatrix}$$

where the $B_{1,r}$ are the Pauli matrices

$$(2) \qquad B_{1,0} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \; B_{1,1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; B_{1,2} = i\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(See **(1)** for a general exposition with applications to Quantum Mechanics.) One formulation, which we shall call the Dirac-Pauli theorem **(2; 3; 1)**, is

THEOREM 1. *If M_1, M_2, M_3, M_4 are 4×4 matrices satisfying*

$$M_r M_s + M_s M_r = 2\delta_{rs} 1_4 \qquad (r, s = 1, 2, 3, 4),$$

then there is a matrix T such that

$$T^{-1} M_r T = B_{2,r-1} \qquad (1 \leqslant r \leqslant 4),$$

and T is unique apart from an arbitrary numerical multiplier.

Various proofs of this theorem are known; those due to Van der Waerden **(4)** and Pauli **(2; 1)** depend on ideas belonging to representation theory; the most elementary proof (ignoring the uniqueness of T) is given by Dirac **(2)**.

Eddington has shown **(5)** that a set of anticommuting 4×4 involution matrices cannot include more than five members, and this was extended by Newman **(6)** to involution matrices of arbitrary order. This had been investigated earlier by Hurwitz **(7)**.

In this note we give a completely elementary proof of Theorem 1 (on the lines of Dirac's proof), giving an explicit calculation of T (Theorem 5 and corollary); the generalization of Theorem 1 to linear transformations of spaces of dimension 2^k is given in Theorem 7. In Theorem 2 we prove a generalization of the Eddington-Newman result in which the restriction to involution matrices is removed.

2. Notation. If V is an n-dimensional vector space, we write $d(V) = n$, and if L is a linear transformation (L.T.) of V into itself we write $d(L) = n$. If M is an $n \times n$ matrix, we write $d(M) = n$; the transpose of M is denoted

Received July 8, 1960.

by M'. The identity mapping in V is denoted by 1 or 1_n, and the same symbols are used to denote the unit matrix.

If λ is an eigenvalue of L, $\mathfrak{E}_\lambda(L)$ denotes the space spanned by the eigenvectors of L belonging to λ. L is called *regular* if 0 is not one of its eigenvalues. A subset S of V is said to be *stable* for L if $L(S) \subset S$. If $d(V) = n$, any ordered set $\{\beta_1, \beta_2, \ldots, \beta_n\}$ which span V is called a *basis* of V; if $\mathfrak{B}$ denotes this basis and c is a non-zero complex number then $c\mathfrak{B}$ denotes the basis $\{c\beta_1, c\beta_2, \ldots, c\beta_n\}$. We say the matrix M represents the linear transformation L in $\mathfrak{B}$ if

$$M = (m_{rs}) \text{ where } L\beta_s = \sum_{r=1}^{n} m_{rs}\beta_r \qquad (1 \leqslant s \leqslant n);$$

this is denoted by $L \sim M$ or by $L \sim M$ (in $\mathfrak{B}$) if the basis is to be made explicit. Plainly if $L \sim M$ (in $\mathfrak{B}$) then $L \sim M$ (in $c\mathfrak{B}$).

L is called an *involution* if $L^2 = 1$ and $L \neq \pm 1$; the involution matrix diag.$(1_n, -1_n)$ is denoted by I_{2n}. L_1 and L_2 are said to *anticommute* if $L_1L_2 = -L_2L_1$.

3. It will be convenient to list some elementary properties of matrices and L.T.'s: it is assumed throughout that the spaces are of finite dimensions; most of the proofs are omitted.

(i) If $d(M) = 2n$ then M anticommutes with I_{2n} if and only if

$$M = \begin{pmatrix} 0 & Q \\ P & 0 \end{pmatrix} \text{ with } d(P) = d(Q) = n,$$

and M is then an involution if and only if $PQ = 1_n$, that is,

$$M = \begin{pmatrix} 0 & P^{-1} \\ P & 0 \end{pmatrix};$$

$$\begin{pmatrix} 0 & X^{-1} \\ X & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & Y^{-1} \\ Y & 0 \end{pmatrix}$$

anticommute if and only if $X^{-1}Y = -Y^{-1}X$. If $L_1, L_2, \ldots, L_{2q}$ are anticommuting involutions then

$$i^q L_1 L_2 \ldots L_{2q}$$

is an involution which anticommutes with each of $L_1, L_2, \ldots, L_{2q}$; (the product of an *odd* set, three or more, will *commute* with the factors).

(ii) If A and B are regular and anticommute then, since

$$\det(AB) = \det(BA)\,(-1)^{d(A)},$$

and since these determinants are not zero, $d(A)$ must be even.

(iii) If L is an involution in V then for every x in V

$$(1 + L)x \in \mathfrak{E}_1(L), \quad (1 - L)x \in \mathfrak{E}_{-1}(L), \quad 2x = (1 + L)x + (1 - L)x,$$

and so V is the direct sum of $\mathfrak{E}_1(L)$ and $\mathfrak{E}_{-1}(L)$; in any basis formed by uniting a basis of $\mathfrak{E}_1(L)$ and a basis of $\mathfrak{E}_{-1}(L)$, $L \sim \text{diag.}(1_m, -1_n)$ for some m, n.

(iv) The basic simple result, to be used repeatedly, is that if S and T are L.T.'s of V, and $ST = kTS$ where k is a non-zero number, and λ is an eigenvalue of T, then S maps $\mathfrak{E}_\lambda(T)$ into $\mathfrak{E}_{\lambda/k}(T)$, and

$$S\{\mathfrak{E}_\lambda(T)\} = \mathfrak{E}_{\lambda/k}(\mathrm{T}) \tag{3}$$

if S is regular. (The proof is trivial: $Tx = \lambda x$ implies $T(Sx) = k^{-1}S(Tx) = k^{-1}\lambda Sx$, and if S is regular we have (since $S(V) = V$ with $d(V) < \infty$) $S^{-1}T = k^{-1}TS^{-1}$, so that S^{-1} maps $\mathfrak{E}_{\lambda/k}(\mathrm{T})$ into $\mathfrak{E}_\lambda(T)$.)

In particular, if an involution L anticommutes with a regular S then

$$S\{\mathfrak{E}_1(L)\} = \mathfrak{E}_{-1}(\mathrm{L}) \quad \text{and} \quad S\{\mathfrak{E}_{-1}(L)\} = \mathfrak{E}_1(L),$$

and it follows from (iii) that $d\{\mathfrak{E}_1(L)\} = d\{\mathfrak{E}_{-1}(L)\} = \frac{1}{2}d(L)$, and that, in a suitable basis of V, $L \sim I_{2n}$ $(n = \frac{1}{2}d(L))$.

(v) If S_1 and S_2 both anticommute with T, then S_1S_2 commutes with T, and so (by (iv)) every eigenspace of T is stable for S_1S_2. In particular, if S_1, S_2, S_3 are anticommuting involutions then

(4) *iS_2S_3 is an involution which maps $\mathfrak{E}_r(S_1)$ onto itself* $(r = \pm 1)$,

(this depends on (i) and (3)).

4. The following generalizes the Eddington-Newman result.

THEOREM 2. *Suppose $L_1, L_2, \ldots, L_{2k}$ are regular anticommuting L.T.'s of V; then 2^k is a divisor of $d(V)$.*

Proof. For $k = 1$ we appeal to § 3 (ii). Now suppose, if possible, that the theorem is true for $k = 1, \ldots, K - 1$ but false for $k = K$. This means that there is a space W in which there are $2K$ regular anticommuting L.T.'s whereas 2^K is not a divisor of $d(W)$. We prove that this leads to a contradiction.

Let Δ be the least value which $d(W)$ can have in the conditions postulated, and suppose W chosen so that $d(W) = \Delta$. Let $\mathfrak{E}_\lambda$ be an eigenspace of L_1; by § 3(v), $\mathfrak{E}_\lambda$ is stable for L_2L_s $(3 \leqslant s \leqslant 2K)$, and the L_2L_s anticommute in $\mathfrak{E}_\lambda$; hence, by the induction hypothesis, $2^{K-1}|d(\mathfrak{E}_\lambda)$. Since $L_r(\mathfrak{E}_\lambda) = \mathfrak{E}_{\pm\lambda}$ for $1 \leqslant r \leqslant 2K$ by (3), the direct sum of $\mathfrak{E}_\lambda$ and $\mathfrak{E}_{-\lambda}$ is stable for all these L_r; thus, in a suitable basis of W,

$$L_r \sim \begin{pmatrix} M_r & P_r \\ 0 & A_r \end{pmatrix} \text{ where } d(M_r) = 2d(\mathfrak{E}_\lambda), \tag{5}$$

which means $d(M_r)$ is divisible by 2^K while $d(L_r)$ is not. Hence $d(A_r)$ is positive and not divisible by 2^K. But, by (5) and the assumption on the L_r, the A_r are regular and they anticommute; thus $d(A_r) \geqslant \Delta = d(L_r)$, which contradicts $d(M_r) > 0$.

It is shown by Newman **(6)** that if $d(V) = 2^n$ then there is a set of $2n + 1$

anticommuting involutions in V (see also § 7 below), but it must not be concluded that an arbitrary set of anticommuting involutions in V which has fewer than $2n+1$ members is part of a maximal set. Thus, with $n = 2$,

$$B_{2,0},\quad B_{2,1},\quad iB_{2.0}B_{2,1}$$

anticommute, but it is easily verified (using § 3(i)) that an involution which anticommutes with the first cannot anticommute with the other two. The same is true if the L.T.'s are regular but not involutory; it is easily verified (using § 3(i)) for the anticommuting matrices

$$\begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&2&0\\0&0&0&-2\end{pmatrix},\quad \begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&2\\0&0&2&0\end{pmatrix},\quad \begin{pmatrix}0&1&0&0\\-1&0&0&0\\0&0&0&4\\0&0&-4&0\end{pmatrix}$$

that if M anticommutes with the first then

$$M = \begin{pmatrix}0&b&0&0\\a&0&0&0\\0&0&0&c\\0&0&d&0\end{pmatrix},$$

and for this to anticommute with the other two, M must vanish.

5. By § 3(iii) every involution in two dimensions has 1 as a simple eigenvalue.

THEOREM 3. *Let* σ_1 *and* σ_2 *be anticommuting involutions in two dimensions and* β_1 *the eigenvector (unique apart from a constant of multiplication) of* σ_1 *belonging to eigenvalue* 1. *Then, apart from an arbitrary numerical multiplier,* $\{\beta_1, \sigma_2(\beta_1)\}$ *is the only basis in which*

$$\sigma_1 \sim \begin{pmatrix}1&0\\0&-1\end{pmatrix} \text{ and } \sigma_2 \sim \begin{pmatrix}0&1\\1&0\end{pmatrix}. \tag{6}$$

Proof. Any basis in which (6) holds must have β_1 (or a numerical multiple of it) for its first member, and for σ_2 to have the matrix assigned in (6) the second member of the basis must be $\sigma_2(\beta_1)$. Conversely, if β_2 is defined as $\sigma_2(\beta_1)$, then $\beta_2 \in \mathfrak{E}_{-1}(\sigma_1)$ by § 3(iv), and $\sigma_2(\beta_2) = \sigma_2^2(\beta_1) = \beta_1$; hence (6) is valid in the basis $\{\beta_1, \beta_2\}$.

THEOREM 4. *Suppose* σ_1 *and* σ_2 *are anticommuting involutions in a two-dimensional space; then, the only regular* L.T.*'s which anticommute with* σ_1 *and* σ_2 *are the numerical multiples of* $\sigma_1\sigma_2$ *and of these the only involutions are* $\pm i\sigma_1\sigma_2$.

Proof. By Theorem 3, we may choose a basis so that (6) holds. A matrix M which anticommutes with the first in (6) has the form

$$\begin{pmatrix}0&p\\q&0\end{pmatrix}$$

by § 3(i), and this anticommutes with the second if and only if $p = -q$, that is,

$$M = p\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \sim p\sigma_1\sigma_2;$$

M is involutory if and only if $p^2 = -1$.

It is a consequence of Theorem 3 and § 3(iv) that if σ_1 and σ_2 are anticommuting involutions in a space V with $d(V) = 2n$ then V is the direct sum of n two-dimensional spaces each stable for σ_1 and σ_2; in a suitable basis of V

$$\sigma_r \sim \text{diag.}(B_{1,r-1}, B_{1,r-1}, \ldots, B_{1,r-1}) \qquad (r = 1, 2). \tag{8}$$

This follows from § 3(iv) whereby if $\{\beta_1, \beta_3, \ldots, \beta_{2n-1}\}$ is a basis of $\mathfrak{E}_1(\sigma_1)$ and $\beta_{2r} = \sigma_2(\beta_{2r-1})$, then β_{2r-1} and β_{2r} span a space stable for σ_1 and σ_2, and (8) will hold in the basis $\{\beta_1, \beta_2, \ldots, \beta_{2n-1}, \beta_{2n}\}$.

We now prove the Dirac-Pauli theorem (this is generalized in § 7).

THEOREM 5. *Let L_0, L_1, L_2, L_3 be anticommuting involutions in the four-dimensional space V; then there is a unique basis (apart from a numerical multiplier) such that $L_r \sim B_{2,r}$ $(r = 0, 1, 2, 3)$, the $B_{2,r}$ being defined by* (1).

Proof. Since

$$B_{2,0} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \qquad B_{2,1} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix},$$

$$B_{2,2} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad B_{2,3} = i\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

we have

$$iB_{2,2}B_{2,3} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \text{ and } iB_{2,3}B_{2,1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

and hence the basic vectors $e_r = (\delta_{r1}, \delta_{r2}, \delta_{r3}, \delta_{r4})$ are completely characterized in terms of the $B_{2,r}$ as follows:

(a) e_1 is the non-zero vector (unique apart from a numerical multiplier), which is common to $\mathfrak{E}_1(B_{2,0})$ and $\mathfrak{E}_1(iB_{2,2}B_{2,3})$,

(b) $e_2 = iB_{2,3}B_{2,1}e_1$, $e_3 = B_{2,1}e_1$, $e_4 = -B_{2,1}e_2 = iB_{2,3}e_1$.

Thus, it is enough to show that (apart from a numerical multiplier) (a′) there is just one non-zero x in $\mathfrak{E}_1(L_0)$ which satisfies $iL_2L_3x = x$, and that if β_1 is such an x, and we define

(b′) $\beta_2 = iL_3L_1\beta_1,\ \beta_3 = L_1\beta_1,\quad \beta_4 = iL_3\beta_1 = -L_1\beta_2,$

then $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ is a basis of V in which $L_r \sim B_{2,r}$ $(0 \leqslant r \leqslant 3)$. Now by § 3(v) $\mathfrak{E}_1(L_0)$ is stable for iL_2L_3 and for iL_3L_1, and these involutions anticommute in $\mathfrak{E}_1(L_0)$. Hence, by Theorem 3, (a′) is true, and if $\beta_2 = iL_3L_1\beta_1$, then

$$iL_2L_3(\beta_1, \beta_2) = (\beta_1, -\beta_2) \qquad \text{and} \qquad iL_3L_1(\beta_1, \beta_2) = (\beta_2, \beta_1);$$

furthermore, $\{\beta_1, \beta_2\}$ span $\mathfrak{E}_1(L_0)$, and so β_3, β_4 may be defined as in (b′), and by § 3(iv) $\{\beta_3, \beta_4\}$ span $\mathfrak{E}_{-1}(L_0)$. Thus, in the basis $\{\beta_1, \beta_2, \beta_3, \beta_4\}$, $L_0 \sim I_2$ and by § 3(i)

$$L_r \sim \begin{pmatrix} 0 & X_r \\ X_r^{-1} & 0 \end{pmatrix} \qquad (1 \leqslant r \leqslant 3).$$

It is therefore enough to verify that $X_r = B_{1,r}$ $(1 \leqslant r \leqslant 3)$. For $r = 1, 2$ this follows from (b′) which implies also that $L_3(\beta_1, \beta_2) = (-i\beta_4, iL_1\beta_1) = (-i\beta_4, i\beta_3)$; this completes the proof.

COROLLARY 1. *Theorem* 1 *follows from Theorem* 5. *If the* L_r *are matrices* M_r (*that is,* V *is the space of number quadruples*), *then* $\beta_1, \beta_2, \beta_3, \beta_4$ *are the columns, in order, of a matrix* T *which satisfies* $M_rT = TB_{2,r}$ $(0 \leqslant r \leqslant 3)$. *These columns are found explicitly from* (a′) *and* (b′) *viz.*

$$(M_0 - 1_4)\beta_1 = (M_2M_3 + i1_4)\beta_1 = 0,$$

and

$$\beta_2 = iM_3M_1\beta_1, \qquad \beta_3 = M_1\beta_1, \qquad \beta_4 = iM_3\beta_1.$$

COROLLARY 2. *If* J_r $(0 \leqslant r \leqslant 3)$ *are anticommuting involutions in* V (*of Theorem* 5) *then there is a regular* L.T., $\mathfrak{T}$, *of* V *such that* $J_r = \mathfrak{T}^{-1}L_r\mathfrak{T}$ $(0 \leqslant r \leqslant 3)$; $\mathfrak{T}$ *is unique apart from a numerical multiplier.*

Proof. By Theorem 5 there is a basis $\mathfrak{B}$ in which $J_r \sim B_{2,r}$ $(0 \leqslant r \leqslant 3)$ and $\mathfrak{B}$ is unique apart from a numerical multiplier. If $L_r \sim M_r$ (in $\mathfrak{B}$) then (by Corollary 1) there is a matrix T, unique apart from a numerical multiplier, with $T^{-1}M_rT = B_r$. Hence the L.T. $\mathfrak{T}$ represented by T in $\mathfrak{B}$ is unique (apart from a numerical multiplier) in satisfying $\mathfrak{T}^{-1}L_r\mathfrak{T} = J_r$ $(0 \leqslant r \leqslant 3)$.

COROLLARY 3. *A regular* L.T. *A which anticommutes with all the* L_r *of Theorem* 5 *must be a numerical multiple of the involution* $L_0L_1L_2L_3$.

Proof. A has to satisfy $AL_rA^{-1} = -L_r$ $(0 \leqslant r \leqslant 3)$; the involution $L_0L_1L_2L_3$ certainly does this, and the result now follows from Corollary 2 with $J_r = -L_r$.

5.1. To illustrate the corollaries to Theorem 5, we prove that (cf. **3**, p. 121) if N_0, N_1, N_2, N_3 are anticommuting 4×4 involution matrices, then there is a skew-symmetric matrix A such that $N_r = A^{-1}N_r'A$ $(0 \leqslant r \leqslant 3)$; A is readily computed.

Since $B_{2,r}'$ $(0 \leqslant r \leqslant 3)$ are anticommuting involutions, there is, by Corollary 1, a matrix T with

$$B'_{2,r} = TB_{2,r}T^{-1} \qquad (0 \leqslant r \leqslant 3),$$

and the columns of T, $\{\beta_1, \beta_2, \beta_3, \beta_4\}$, are found from $B_{2,0}\beta_1 = -iB_{2,2}B_{2,3}\beta_1 = \beta_1$, $\beta_2 = -iB_{2,3}B_{2,1}\beta_1$, $\beta_3 = B_{2,1}\beta_1$, $\beta_4 = -iB_{2,3}\beta_1$; these give $\beta_1 = e_2$, $\beta_2 = -e_1$, $\beta_3 = -e_4$, $\beta_4 = e_3$, that is

(a) $$T = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

Since the N_r are anticommuting involutions, one could compute by Corollary 1 a matrix Q with

$$QN_rQ^{-1} = B_{2,r} \qquad (0 \leqslant r \leqslant 3).$$

We now have

$$QN_rQ^{-1} = (TB_{2,r}T^{-1})' = (TQN_rQ^{-1}T^{-1})', \text{ that is, } N_r = A^{-1}N_r'A,$$

where A, equal to $Q'T'Q$, is skew-symmetric because T is.

As a second illustration, we find a formula for all sets of four anticommuting 4×4 involution matrices with are skew-symmetric. This means (by Theorem 5) finding a formula for all matrices P which satisfy

$$PB_{2,r}P^{-1} = -(P^{-1})'B'_{2,r}P', \qquad (0 \leqslant r \leqslant 3);$$

using the illustration above, this means simply that $T^{-1}P'P$ anticommutes with $B_{2,r}$ $(0 \leqslant r \leqslant 3)$. By Corollary 3 this is equivalent to the statement that $T^{-1}P'P$ is a numerical multiple of

$$\begin{pmatrix} 0 & 1_2 \\ -1_2 & 0 \end{pmatrix}$$

which, by (a), means that $P'P$ is a numerical multiple of

$$\left(\begin{array}{cc:cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ \hdashline 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{array}\right)$$

that is, of $B_{2,1}$. Bearing in mind that the eigenvalues of $B_{2,1}$ are ± 1 it is easy to see that

$$B_{2,1} = \tfrac{1}{2}M'M, \text{ where } M = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ i & 0 & -i & 0 \\ 0 & i & 0 & i \end{pmatrix},$$

and hence that P has the form $c\Omega M$ where c is an arbitrary number and Ω an arbitrary orthogonal matrix (that is, $\Omega\Omega' = 1_4$). Thus the formula

$$J_r = \Omega M B_{2,r} M^{-1} \Omega' \qquad (0 \leqslant r \leqslant 3)$$

gives the required sets of involutions.

5.2. The result corresponding to (8) is as follows:

THEOREM 6. *Suppose L_0, L_1, L_2, L_3 are anticommuting involutions of V and $d(V) > 4$; then V is the direct sum of four-dimensional subspaces each stable for all the L_r, and in a suitable basis of V*

$$L_r \sim \text{diag.}(B_{2,r}, B_{2,r}, \ldots, B_{2,r}) \qquad (0 \leqslant r \leqslant 3).$$

Proof. Write S_1 for iL_2L_3 and S_2 for iL_3L_1. Then, as in the proof of Theorem 5, $\mathfrak{E}_1(L_0)$ is the direct sum of two-dimensional spaces, say $W_1, W_2, \ldots, W_q$, each of which is stable for S_1 and S_2 as well as for L_0. If W_r' is defined as $L_1(W_r)$, then by § 3(iv), $W_r' \subset \mathfrak{E}_{-1}(L_0)$ and W_r' is stable for S_1 and S_2. Thus the direct sum of W_r and W_r' is stable for L_0, L_1, S_1, and S_2; it is therefore stable for L_2 and L_3. It now follows from Theorem 5 that in this subspace of V there is a basis in which $L_s \sim B_{2,s}$. Since this holds for $1 \leqslant s \leqslant q$, and V is the direct sum of $\mathfrak{E}_1(L_0)$ and $\mathfrak{E}_{-1}(L_0)$, this completes the proof.

6. If a scalar product is defined in the spaces considered in Theorems 3 and 5, then the conclusions can be further particularized if the σ_r and the L_r are unitary (an involution is unitary if and only if it is hermitean). The modification is that the basis can be chosen orthonormal. This will follow in Theorem 3 from the fact that $\mathfrak{E}_1(\sigma_1)$ and $\mathfrak{E}_{-1}(\sigma_1)$ are orthogonal and that if $||\beta_1|| = 1$ then $||\beta_2|| = ||\sigma_2(\beta_1)|| = 1$. In the case of Theorem 5, the S_r defined in Theorem 6 will be unitary if the L_r are unitary, and consequently, as above β_1, β_2 can be chosen orthonormal in $\mathfrak{E}_1(L_0)$; it then follows from (b′) in Theorem 5 that β_3 and β_4 are orthonormal in $\mathfrak{E}_{-1}(L_0)$ while the two spaces $\mathfrak{E}_1(L_0)$ and $\mathfrak{E}_{-1}(L_0)$ are orthogonal. Similarly, if the matrices M_r in Theorem 1 are hermitean, then T can be chosen unitary. Since the $B_{2,r}$ are hermitean, it follows that the M_r are hermitean if and only if there is a unitary matrix U with $M_r = U^{-1}B_{2,r}U$ $(0 \leqslant r \leqslant 3)$.

7. In this section we generalize Theorem 5. Having defined

$$B_{1,0} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \; B_{1,1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; B_{1,2} = iB_{1,0}B_{1,1} = i\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

we now define, inductively, for every positive integer n a set of $2n+1$ matrices as follows:

$$B_{n,0} = \begin{pmatrix} 1_{2^{n-1}} & 0 \\ 0 & -1_{2^{n-1}} \end{pmatrix},\quad B_{n,r} = \begin{pmatrix} 0 & B_{n-1,r-1} \\ B_{n-1,r-1} & 0 \end{pmatrix} (1 \leqslant r \leqslant 2n-1),$$

$$B_{n,2n} = i^n B_{n,0}B_{n,1}\ldots B_{n,2n-1}.$$

By § 3(i) it follows at once that, because the $B_{1,r}$ are involutions, the $2n+1$ involutions $B_{n,r}$ anticommute.

LEMMA.

$$\text{(9)}\qquad B_{n,2n} = i\begin{pmatrix} 0 & 1_{2^{n-1}} \\ -1_{2^{n-1}} & 0 \end{pmatrix},\ \text{that is, } B_{n,0}B_{n,1}\ldots B_{n,2n-1}B_{n,2n} = (-i)^n 1_{2^n}.$$

Proof. The equivalence of the two statements in (9) follows from the definition of $B_{n,2n}$ which gives $i^n B_{n,0}B_{n,1}\ldots B_{n,2n} = (B_{n,2n})^2 1_{2^n}$. The lemma is obvious when $n = 1$. Suppose $q > 1$ and that the lemma has been proved for $n = q-1$. By the definition of $B_{q,2q}$,

$$B_{q,2q} = i^q\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & B_{q-1,0} \\ B_{q-1,0} & 0 \end{pmatrix}\begin{pmatrix} 0 & B_{q-1,1} \\ B_{q-1,1} & 0 \end{pmatrix}\ldots\begin{pmatrix} 0 & B_{q-1,2q-2} \\ B_{q-1,2q-2} & 0 \end{pmatrix}$$

$$= i^q\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & B_{q-1,0}B_{q-1,1}\ldots B_{q-1,2q-2} \\ B_{q-1,0}B_{q-1,1}\ldots B_{q-1,2q-2} & 0 \end{pmatrix},$$

and by the induction hypothesis this gives

$$B_{q,2q} = i^q\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & (-i)^{q-1}1_{2^{q-1}} \\ (-i)^{q-1}1_{2^{q-1}} & 0 \end{pmatrix} = i\begin{pmatrix} 0 & 1_{2^{q-1}} \\ -1_{2^{q-1}} & 0 \end{pmatrix}.$$

THEOREM 7. *Suppose $L_0, L_1, \ldots, L_{2q-1}$ is a set of $2q$ anticommuting involutions in V and $d(V) = 2^q$; then, defining $L_{2q} = i^q L_0 L_1 \ldots L_{2q-1}$, there is a basis $\mathfrak{B}$ in which $L_r \sim B_{q,r}$ $(0 \leqslant r \leqslant 2q)$, and $\mathfrak{B}$ is unique apart from a numerical multiplier. The only regular* L.T.*'s of V which anticommute with $L_0, L_1, \ldots, L_{2q-1}$ are the numerical multiples of L_{2q}, and, of these, $\pm L_{2q}$ are the only involutions.*

Proof (by induction on q). Theorems 3 and 4 justify Theorem 7 when $q = 1$. Suppose the theorem is true when $q = n > 1$ and let $L_0, L_1, \ldots, L_{2n+1}$ be a set of $2n+2$ anticommuting involutions in V with $d(V) = 2^{n+1}$.

We first assume that V *has* a basis $\mathfrak{B}$ in which $L_r \sim B_{n+1,r}$ $(0 \leqslant r \leqslant 2n+2)$, and show that $\mathfrak{B}$ is essentially unique (that is, that any other basis with the same property must be $c\mathfrak{B}$). Define

$$L^*_s = iL_s L_{2n+2} \qquad (1 \leqslant s \leqslant 2n+1);$$

by § 3(v) the L^*_s are anticommuting involutions for which $\mathfrak{E}_1(L_0)$ and $\mathfrak{E}_{-1}(L_0)$ are stable; denote by L^{**}_s the L.T. of $\mathfrak{E}_1(L_0)$ effected by L^*_s. The involutions L^{**}_s anticommute in $\mathfrak{E}_1(L_0)$ which has dimension 2^n, and so, by the induction hypothesis, $\mathfrak{E}_1(L_0)$ has a basis $\mathfrak{B}_1 = \{\beta_1, \beta_2, \ldots, \beta_{2^n}\}$ (unique apart from a

https://doi.org/10.4153/CJM-1961-050-2 Published online by Cambridge University Press

numerical multiplier) in which $L^{**}_s \sim B_{n,s-1}$ $(1 \leqslant s \leqslant 2n)$. But, in the postulated basis $\mathfrak{B}$, $L_0 \sim I_{2^n}$, and

$$L_s^* \sim i\begin{pmatrix} 0 & B_{n,s-1} \\ B_{n,s-1} & 0 \end{pmatrix} i\begin{pmatrix} 0 & 1_{2^n} \\ -1_{2^n} & 0 \end{pmatrix} = \begin{pmatrix} B_{n,s-1} & 0 \\ 0 & B_{n,s-1} \end{pmatrix} \qquad (1 \leqslant s \leqslant 2n)$$

Hence $\beta_1, \beta_2, \ldots, \beta_{2^n}$ are the first 2^n members of $\mathfrak{B}$. Since

$$L_{2n+2} \sim i\begin{pmatrix} 0 & 1_{2^n} \\ -1_{2^n} & 0 \end{pmatrix}$$

(in $\mathfrak{B}$), it follows now that if $\mathfrak{B} = \{\beta_1, \beta_2, \ldots, \beta_{2^{n+1}}\}$ then

$$\beta_{r+2^n} = iL_{2n+2}\beta_r \qquad (1 \leqslant r \leqslant 2^n),$$

and so $\mathfrak{B}$ is determined completely (apart from a numerical multiplier) by $L_0, L_1, \ldots, L_{2n+1}$.

We now define $\mathfrak{B}'$ as $\{\mathfrak{B}_1, iL_{2n+2}\mathfrak{B}_1\}$ and proceed to prove that $L_r \sim B_{n+1,r}$ (in $\mathfrak{B}'$) for $0 \leqslant r \leqslant 2n+2$. Since $\mathfrak{B}_1$ spans $\mathfrak{E}_1(L_0)$ and $L_{2n+2}(\mathfrak{B}_1)$ spans $\mathfrak{E}_{-1}(L_0)$ (§ 3(iv)), it follows that in $\mathfrak{B}'$

$$L_0 \sim \begin{pmatrix} 1_{2^n} & 0 \\ 0 & -1_{2^n} \end{pmatrix}, \; L_{2n+2} \sim i\begin{pmatrix} 0 & 1_{2^n} \\ -1_{2^n} & 0 \end{pmatrix} \text{ and}$$

$$iL_sL_{2n+2} \sim \begin{pmatrix} B_{n,s-1} & 0 \\ 0 & X_s \end{pmatrix} \qquad (1 \leqslant s \leqslant 2n),$$

where the exact form of X_s need not concern us. These imply

$$L_s = (L_sL_{2n+2})L_{2n+2} = \begin{pmatrix} B_{n,s-1} & 0 \\ 0 & X_s \end{pmatrix}\begin{pmatrix} 0 & 1_{2^n} \\ -1_{2^n} & 0 \end{pmatrix} = \begin{pmatrix} 0 & B_{n,s-1} \\ -X_s & 0 \end{pmatrix};$$

and since L_s anticommutes with L_0 it now follows by § 3(i) that

$$L_s \sim \begin{pmatrix} 0 & B_{n,s-1} \\ B_{n,s-1} & 0 \end{pmatrix} = B_{n+1,s} \qquad \text{for } s = 1, 2, \ldots, 2n, 2n+2.$$

To verify that the formula holds also when $s = 2n+1$, we note that $L_{2n+2} = i^{n+1}L_0 \ldots L_{2n+1}$ (by definition) and $L_{2n+2} \sim i^{n+1}B_{n+1,0}B_{n+1,1} \ldots B_{n+1,2n+1}$ from the known matrix representing L_{2n+2}. This proves $L_{2n+1} \sim B_{n+1,2n+1}$.

Finally, consider matrices M which satisfy

$$(10) \qquad M^{-1}(-B_{q,s})M = B_{qs} \qquad (0 \leqslant s \leqslant 2q-1).$$

The columns of such an M are, in order, the members of a basis (of the space of number 2^q-ples) in which the $(-B_{q,s})$ are represented by the $B_{q,s}$ respectively. Since the $2q$ involutions $-B_{q,1}, -B_{q,2}, \ldots, -B_{q,2q-1}$ anticommute, it follows from the first part of this theorem that such a basis is essentially unique. Since $M = B_{q,2q}$ satisfies (10), it now follows that $M = cB_{q,2q}$, with c an arbitrary number, is the complete solution of (10) and that M is an involution if and only if $c^2 = 1$. Since the L_r are represented by the $B_{q,r}$, this completes the proof of the theorem.

References

1. R. H. Good, *Properties of the Dirac matrices*, Rev. Mod. Phys., *27* (1955), 187.
2. P. A. M. Dirac, *The quantum theory of the electron*, Proc. Roy. Soc. A., *117* (1928), 616.
3. W. Pauli, *Contributions mathématiques à la théorie de Dirac*, Ann. Inst. Henri Poincaré, *6* (1936), 109.
4. B. L. Van der Waerden, *Die Gruppentheoretische Methode in der Quantenmechanik* (Berlin, 1932), 55.
5. A. S. Eddington, *On sets of anticommuting matrices*, J. London Math. Soc., *17* (1932), 58.
6. M. H. A. Newman, *Note on an algebraic theorem of Eddington*, J. London Math. Soc., *17* (1932), 93.
7. A. Hurwitz, *Ueber die Komposition der Quadratischen Formen*, Math. Annalen, *88* (1923), 1.

University College
London