Lectures on Riemann matrices

By

C.L. Siegel

Tata Institute of Fundamental Research, Bombay
1963

Lectures on Riemann matrices

By

C.L. Siegel

Notes by

S. Raghavan

and

S.S. Rangachari

Tata Institute of Fundamental Research
Bombay
1963

Forword

The following lecture notes were carefully prepared by Dr.S. Raghavan and Dr.S.S. Rangachari. I thank them for their most valuable collaboration.

Carl Ludwig Siegel

Contents

1 Chapter 1 **1**

1 Introduction: Abelian Functions 1
2 The commutator-algebra of a R-matrix 5
3 Division algebras over $\mathbb{Q}$ with a positive involution . . . 13
4 Cyclic algebras 27
5 Division algebras over $\mathbb{Q}$... 32
6 Positive involutions of the second kind in division algebras 36
7 Existence of R-matrices with given commutator-algebra . 41
8 Modular groups associated with Riemann matrices . . . 81

Chapter 1

1 Introduction: Abelian Functions

1

In this course of lectures, we shall be concerned with a systematic study of Riemann matrices which arise in a natural way from the theory of abelian functions. This introductory article will be devoted to explaining this connections.

Let $u_1, \ldots, u_n$ be n independent complex variables and 1et $u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$. We shall denote by $\mathbb{C}^n$, the n-dimensional complex euclidean space and by $\mathbb{C}$, the field of complex numbers. Let $f(u)$ be an *abelian function* of u; in other words, $f(u)$ is a complex-valued function defined and meromorphic in $\mathbb{C}^n$ and having 2n periods $\omega_1, \ldots, w_{2n}$ linearly independent over the field of real numbers (i.e. for $1 \leq i \leq 2n$, $f(u + \omega_i) = f(u)$). We suppose further that $f(u)$ is a *non-degenerate* abelian function i.e. there does not exist any complex linear transformation of the variables $u_1, \ldots, u_n$ such that $f(u)$ can be brought to depend on strictly less than n complex variables.

The periods of $f(u)$ form a lattice Γ in $\mathbb{C}^n$, which we may assume, without loss of generality, to be generated by $\omega_1, \ldots, \omega_{2n}$ over the ring $\mathbb{Z}$ of rational integers. The matrix $P = (\omega_1 \omega_2 \ldots \omega_{2n})$ of n rows and $2n$ columns is called a *period-matrix* of the lattice Γ. Any other period-matrix P_1 of Γ is of the form $P\,U$ where U is unimodular (i.e. U is a rational integral matrix of determinant ± 1).

The abelian functions admitting all elements of Γ as periods, form a field $\mathbb{G}$. It is known that there exist $n + 1$ abelian functions $f_0(u)$,

2 $f_1(u), \ldots, f_n(u)$ in $\mathbb{G}$ such that $f_1(u), \ldots, f_n(u)$ are algebraically independent over $\mathbb{C}$ (and, in fact, even analytically independent), $f_0(u)$ depends algebraically upon $f_1(u), \ldots, f_n(u)$ and further

$\mathbb{G} = \mathbb{C}(f_0(u), \ldots, f_n(u))$. In other words, $\mathbb{G}$ is an algebraic function field of n variables over $\mathbb{C}$.

Let now $\mathscr{L}$ be another field of abelian functions of the form $g(u) = f(K^{-1}u)$ for $f(u) \in \mathbb{G}$ and fixed complex nonsingular matrix K. Let us further, suppose that $\mathscr{L}$ has period-lattice Δ contained in Γ. Then it is easy to show that $\mathscr{L}$ is an algebraic extension of $\mathbb{G}$. Moreover, if Q is a period-matrix of Δ, then, on the one hand, $Q = KPU$ for a unimodular U and, on the other hand, $Q = PG_1$ for a nonsingular rational integral matrix G_1. Thus we have

$$KP = PG \tag{1}$$

with complex nonsingular $\underline{K}$ and rational integral G. We call any such K, a *complex multiplication* of P and G, a *multiplier* of P. Our object is to study the nature of the set of K and G satisfying the matrix equation (1). To this end, we first relax our conditions and ask for all rational $2n$-rowed square matrices M satisfying the condition

$$KP = PM \tag{2}$$

with a suitable complex matrix K. It is easy to verify that the set of such M is an algebra $\mathfrak{M}$ of finite rank over the field $\mathbb{Q}$ of rational numbers. We denote this abstract algebra by $\mathfrak{M}$, while the set of matrices M give a matrix representation of $\mathfrak{M}$ which we denote by $(\mathfrak{M})$.

3 For the period-matrix P, there exists a rational $2n$-rowed alternate non-singular matrix A such that

$$i)\ PA^{-1}P' = 0 \tag{3}$$

and $$ii)\ H = \sqrt{-1}PA^{-1}\overline{P}' > 0 \text{ (i.e. positive hermitian)}$$

We call A, a *principal matrix* for P.

Definition . *Any complex matrix P of n rows and $2n$ columns satisfying* (3) *for some principal matrix A is called a (n-rowed)* Riemann matrix.

Conditions (3) are known as Riemann's *period relations*. In the case when $A = \left(\begin{smallmatrix} 0 & E \\ -E & 0 \end{smallmatrix}\right)$ (E being the n-rowed identity matrix), conditions (3) were given by Riemann [16] as precisely the conditions to be satisfied by the periods of a normalized complete system of abelian integrals of the first kind on a Riemann surface of genus n. It was shown by Poincare that conditions (3) are necessary and sufficient for P to be a period-matrix of a nondegenerate abelian function.

Let now $Q = \left(\frac{P}{\overline{P}}\right)$. Then conditions (3) may be rewritten as

$$i\, Q\, A^{-1}\, \overline{Q}' \left(\begin{smallmatrix} H & 0 \\ 0 & -\overline{H} \end{smallmatrix}\right) \quad (i = \sqrt{-1}) \tag{4}$$

with H positive hermitian. If $W = iQA^{-1}\overline{Q}'$, then W and therefore Q are nonsingular. We may now reformulate (2) as

$$TQ = QM \tag{5}$$

where $T = \left(\begin{smallmatrix} K & 0 \\ 0 & \overline{K} \end{smallmatrix}\right)$.

Following H. Weyl, we introduce the $2n$-rowed matrix $L = \left(\begin{smallmatrix} -iE & 0 \\ 0 & iE \end{smallmatrix}\right)$ and consider, instead of P, the matrix

$$R = Q^{-1}LQ. \tag{6}$$

Under the transformation $P \to DP$ or equivalently $Q \to \left(\begin{smallmatrix} D & 0 \\ 0 & \overline{D} \end{smallmatrix}\right) Q$ 4
(with arbitrary complex nonsingular D), R remains unchanged. If P is a period-matrix, this has the significance that R as defined by (6) is independent of the choice of the differentials $du_1, \ldots, du_n$ of the first kind on the abelian variety associated with P.

The advantage in working with R is that in the first place R is real as we shall see presently and, further, that equation (5) may be written simpler as

$$RM = MR \tag{7}$$

using the fact that $LT = TL$. Thus M has to be just a $2n$-rowed rational matrix commuting with R. Conversely, if M is such a matrix, then defining $T = QMQ^{-1}$, we have $LT = TL$. But, from the form of L, we see that $T = \left(\begin{smallmatrix} K & 0 \\ 0 & K_1 \end{smallmatrix}\right)$ with n-rowed square matrices K and K_1. But $TQ = QM$

gives $KP = PM = \overline{\overline{P}M} = \overline{K}_1 P$ which, in turn, leads to $K = \overline{K}_1$ (since P is of rank n). Thus the rational solutions M of (7) are the same as those of (5).

Proposition 1. *The matrix R defined by* (6) *has the following properties:*

(*i*) *R is real*

(*ii*) $R^2 = -E$(*E being the* 2*n-rowed identity matrix*)

and (*iii*) $S = AR$ *is positive symmetric*.

Conversely, any 2*n-rowed rational matrix having properties (i), (ii)*
5 *and (iii) leads to a Riemann matrix P which is uniquely determined upto a left-sided nonsingular factor and P has A for a principal matrix.*

Proof. Let $V = \left(\begin{smallmatrix} 0 & E \\ E & 0 \end{smallmatrix}\right)$ with E being the n-rowed identity matrix. Since $\overline{Q} = VQ$ and $V^{-1}\overline{L}V = L$, we have $\overline{R} = \overline{Q}^{-1}\overline{L}\,\overline{Q} = Q^{-1}V^{-1}\overline{L}VQ = R$, which proves (i). From $L^2 = -E$, (ii) follows. To prove (iii), we set $F = iQA^{-1}\overline{Q}' = \left(\begin{smallmatrix} H & 0 \\ 0 & -\overline{H} \end{smallmatrix}\right)$. Then $F = \overline{F}'$ and $S = AR = AQ^{-1}LQ = i\overline{Q}'F^{-1}LQ = \overline{Q}'F^{-1}\left(\begin{smallmatrix} E & 0 \\ 0 & -E \end{smallmatrix}\right)Q$. But $F^{-1}\left(\begin{smallmatrix} E & 0 \\ 0 & -E \end{smallmatrix}\right) = \left(\begin{smallmatrix} H^{-1} & 0 \\ 0 & \overline{H}^{-1} \end{smallmatrix}\right)$ is positive hermitian and so is its transform S. Since S is real, our assertion (iii) is proved.

Conversely, let R have the properties (i), (ii) and (iii). From (ii), the eigen-values of R are $+i$ and $-i$ and they occur with the same multiplicity n, since the characteristic equation of R is of degree $2n$ and has real coefficients. Thus it may be seen that there is a complex non-singular matrix C such that $R = C^{-1}LC$. If C_0 also satisfies $C_0^{-1}LC_0 = R$, then $C_0 = \left(\begin{smallmatrix} B_1 & 0 \\ 0 & B_2 \end{smallmatrix}\right)C$ with complex n-rowed non-singular matrices B_1 and B_2. Now from (i), $C^{-1}LC = \overline{C}^{-1}\overline{L}\,\overline{C} = (V\overline{C})^{-1}L(V\overline{C})$ since $\overline{L} = V^{-1}LV$ so that $V\overline{C} = \left(\begin{smallmatrix} B_1 & 0 \\ 0 & B_2 \end{smallmatrix}\right)C$ or $\overline{C} = \left(\begin{smallmatrix} 0 & B_2 \\ B_1 & 0 \end{smallmatrix}\right)C$. Splitting up C as $\left(\begin{smallmatrix} C_1 \\ C_2 \end{smallmatrix}\right)$ with n-rowed C_1, we have $\overline{C}_1 = B_2C_2$ and $\overline{C}_2 = B_1C_1$. We may now choose $Q = \left(\begin{smallmatrix} C_1 \\ B_2\ C_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} E & 0 \\ 0 & B_2 \end{smallmatrix}\right)\left(\begin{smallmatrix} C_1 \\ C_2 \end{smallmatrix}\right)$. Then $Q^{-1}LQ = R$ and if
6 we denote C_1 as P, $Q = \left(\begin{smallmatrix} P \\ \overline{P} \end{smallmatrix}\right)$. We shall prove that P is a Riemann matrix having A for a principal matrix. In fact, from (iii), we have $AQ^{-1}LQ = \overline{Q}'F^{-1}\left(\begin{smallmatrix} E & 0 \\ 0 & -E \end{smallmatrix}\right)Q$ is positive hermitian, where $F = iQA^{-1}\overline{Q}'$.

But then this means $F^{-1}\left(\begin{smallmatrix} E & 0 \\ 0 & -E \end{smallmatrix}\right)$ is hermitian and positive. Therefore, $\left(\begin{smallmatrix} E & 0 \\ 0 & -E \end{smallmatrix}\right)F$ is again positive hermitian. Writing $F = \left(\begin{smallmatrix} F_1 & F_2 \\ \overline{F}_2' & F_3 \end{smallmatrix}\right)$ we have $\left(\begin{smallmatrix} F_1 & F_2 \\ -\overline{F}_2' & -F_3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \overline{F}_1' & -F_2 \\ \overline{F}_2' & -\overline{F}_3' \end{smallmatrix}\right)$. Thus $F_2 = 0$ and $F_1, -F_3$ are positive hermitian. Writing $F = \left(\begin{smallmatrix} H & 0 \\ 0 & H_1 \end{smallmatrix}\right)$ where $H, -H_1$ are positive hermitian, it is trivial to see $H_1 = -\overline{H}$. Thus our proposition is completely proved.

For the sake of brevity, we shall call a matrix R having properties (i), (ii) and (iii) mentioned in Proposition 1, a *R-matrix*. A real matrix satisfying just condition (iii) is referred to by H. Weyl [27] as a "generalized Riemann matrix". We shall call the matrix A, a 'principal matrix' for R, too.

□

2 The commutator-algebra of a R-matrix

In the last section we reduced the problem of finding the set of rational matrices M satisfying (2) for a suitable complex K, to that of finding all $2n$-rowed rational matrices M which commute with a $2n$-rowed R-matrix R. We may now forget the period matrix P which gave rise to R and work with R instead. As we remarked, the set of such commutators M of R is an algebra $(\mathfrak{M})$ of finite rank over $\mathbb{Q}$.

We shall now see that in $(\mathfrak{M})$, we have an involution $M \to M^*$; this involution is known as the *Rosati involution*. Further, it is a *positive involution* in the sense that for any $M \in (\mathfrak{M})$, the trace $\sigma(MM^*)$ of MM^* 7
is a positive rational number unless $M = 0$.

(For a complex square matrix X, we denote the *trace* by $\sigma(X)$ and the *determinant* by $|X|$).

Proposition 2. *We have in $\mathfrak{M}$, a positive involution.*

Proof. For any $2n$-rowed complex square matrix W, define

$$W^* = A^{-1}W'A.$$

Then it is easy to verify that

$$(W_1 \pm W_2)^* = A^{-1}(W_1 \pm W_2)'A = W_1^* \pm W_2^*$$

$$(cW_1)^* = cW_1^* \text{ for any } c \in \mathbb{C}. \tag{8}$$
$$(W_1W_2)^* = A^{-1}W_2'W_1'A = W_2^*W_1^*$$
$$(W^*)^* = A^{-1}(A^{-1}W'A)'A = W$$

If $M \in (\mathfrak{M})$, then $MR = RM$ and by (8), $M^*R^* = R^*M^*$. But $R^* = A^{-1}R'A = -A^{-1}S = -R$. Thus $M^*R = RM^*$. Further M^* is a rational matrix and therefore $M^* \in (\mathfrak{M})$. We now obtain from (8) that the mapping $M \to M^*$ of $(\mathfrak{M})$ is an anti-automorphism of order 2, i.e. an involution.

Clearly $\sigma(MM^*) = \sigma(MA^{-1}M'A) = \sigma(MRS^{-1}M'SR^{-1}) = \sigma(RMS^{-1}M'SR^{-1}) = \sigma(MS^{-1}M'S) = \sigma(MC^{-1}C'^{-1}M'C'C) = \sigma(CMC^{-1}C'^{-1}M'C')$ where C is a real nonsingular matrix such that $S = C'C$. Now setting $G = CMC^{-1}$, we have $\sigma(MM^*) = \sigma(GG')$ which is strictly positive for $G \neq 0$ and zero for $G = 0$. Equivalently, $\sigma(MM^*) > 0$ for $M \neq 0$ in $(\mathfrak{M})$ and $\sigma(MM^*) = 0$ for M=0.

8 We shall see later that the property of $(\mathfrak{M})$ mentioned in Proposition 2 serves to characterise the algebra of multiplications of a Riemann matrix. More precisely, we shall prove that, except in some very special cases, any matrix algebra over $\mathbb{Q}$ carrying a positive involution can be realized as the algebra of multiplications of a Riemann matrix. To this end, we need to prove some preliminary results.

A $2n$-rowed R-matrix R is said to be *reducible*, if there exists a rational $2n$-rowed non-singular matrix C_1 such that

$$C_1^{-1}RC_1 = \begin{pmatrix} R_1 & R_{12} \\ 0 & R_2 \end{pmatrix} \tag{9}$$

where R_1 is a matrix of $n_1 (< 2n)$ rows and n_1 columns. Otherwise, we say that R is *irreducible*.

Let us remark that if R is a reducible R-matrix, it is not a priori obvious from the form (9) of $C_1^{-1}RC_1$ whether R_1 and R_2 are again R-matrices and whether atleast n_1 is even. We obtain clear information about this from □

Theorem 1 (Poincare, [12])**.** *If R is a $2n$-rowed reducible R-matrix then there exists a rational non-singular matrix C such that*

$$C^{-1}RC = \begin{pmatrix} R_1 & 0 \\ 0 & R_2 \end{pmatrix} \tag{10}$$

where R_1 and R_2 are again R-matrices of $2r$ and $2(n-r)$ rows respectively.

Proof. We may take R already in the form $\begin{pmatrix} R_1 & R_{12} \\ 0 & R_2 \end{pmatrix}$, without loss of generality. Let n_1 and $n_2(=2n-n_1)$ be the number of rows of R_1 and R_2 **9** respectively and let E_i be the identity matrix of n_i rows $(i=1,2)$. It is then enough to find first a suitable rational X such that for $C=\begin{pmatrix} E_1 & X \\ 0 & E_2 \end{pmatrix}$, we have $C^{-1}RC$ in the form (10). Now

$$C^{-1}RC=\begin{pmatrix} E_1 & -X_2 \\ 0 & E_2 \end{pmatrix}\begin{pmatrix} R_1 & R_{12} \\ 0 & R_2 \end{pmatrix}\begin{pmatrix} E_1 & X \\ 0 & E_2 \end{pmatrix}=\begin{pmatrix} R_1 & R_{12}+R_1X-XR_2 \\ 0 & R_2 \end{pmatrix}.$$

If X is rational and satisfies $R_{12}+R_1X-XR_2=0$, we will be through. Breaking up A as $\begin{pmatrix} A_1 & A_{12} \\ -A'_{12} & A_2 \end{pmatrix}$ and S as $\begin{pmatrix} S_1 & S_{12} \\ S'_{12} & S_2 \end{pmatrix}$ in a similar way, we see that A_1 is a nonsingular alternate matrix, since $S_1=A_1R_1$ is positive symmetric. Thus n_1 is even and let $n_1=2r$ (say). Further from $A_1R_1=S_1=-R'_1A_1$, we have

$$A_1R_{12}+A_{12}R_2=S_{12}=(-A'_{12}R_1)'=-R'_1A_{12}=A_1R_1A_1^{-1}A_{12}.$$

Setting $X=-A_1^{-1}A_{12}$, we have a rational matrix X satisfying $R_{12}+R_1X-XR_2=0$.

To complete the proof, we first remark that if R is replaced by $C^{-1}RC$, then A, S and M have respectively to be replaced by $C'AC$, $C'SC$ and $C^{-1}MC$. Now

$$C'AC=\begin{pmatrix} E_1 & 0 \\ X' & E_2 \end{pmatrix}\begin{pmatrix} A_1 & A_{12} \\ -A'_{12} & A_2 \end{pmatrix}\begin{pmatrix} E_1 & X \\ 0 & E_2 \end{pmatrix}=\begin{pmatrix} A_1 & 0 \\ 0 & A_3 \end{pmatrix}$$

where $A_3=A_2-A'_{12}A_1^{-1}A_{12}$ is again an alternate $2(n-r)$-rowed nonsingular matrix. Further from the form of $C'AC$ and $C^{-1}RC$, it is clear that $C'SC=\begin{pmatrix} S_1 & 0 \\ 0 & S_2 \end{pmatrix}$ where S_1 and S_2 are positive symmetric matrices of $2r$ and $2(n-r)$ rows respectively. From $R^2=-E$, we have $R_1^2=-E_1$, **10** $R_2^2=-E_2$ and from $C'SC>0$, we see that $A_1R_1=S_1$ and $A_3R_2=S_2$ are again positive symmetric. Thus R_1 and R_2 are again R-matrices. □

Remarks. (1) Theorem 1 was proved by Poincare only in the special case when the underlying abelian variety is the Jacobian of a Riemann surface of genus n (see also p.133, [26]).

(2) If R is reducible and $MR = RM$, then although $C^{-1}MC$ commutes with $C^{-1}RC$, it is not necessary that $C^{-1}MC$ should reduce to the form (10).

(3) In terms of period matrices, the transformation $R \to C^{-1}RC$ corresponds to the transformation $P \to PC$ where P is a period matrix associated to R (by Proposition 1). From (10), we can prove that $PC = \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}$ where P_1 and P_2 are period matrices of r and $n - r$ rows respectively. The field of abelian functions having PC for a period matrix is the composite of the fields of abelian functions having P_1 and P_2 for period matrices respectively.

Applying the reduction above successively, we can split R into irreducible R-matrices.

If $A, B, C, \ldots$ are finitely many square matrices, then $[A, B, C, \ldots]$ shall stand for the direct sum of $A, B, C, \ldots$. With this notation, we can find by Theorem 1, a rational $2n$-rowed non-singular matrix C such that

$$C^{-1}RC = [R_1, R_2, \ldots], \tag{11}$$

and correspondingly

$$C'AC = [A_1, A_2, \ldots].$$

11 If two of the matrices R_i occurring on the right hand side in (11) are equivalent, say $R_2 = C_1^{-1}R_1C_1$, for a rational non-singular C_1, then, replacing C by $C\begin{pmatrix} E_1 & 0 & 0 \\ 0 & C_1^{-1} & 0 \\ 0 & 0 & E \end{pmatrix}$, we could suppose that already $R_1 = R_2$. In this process of changing C, A_2 gets replaced by $C_1'A_2C_1$. Now if $C_1'A_2C_1$ is not equal to A_1, we could change the matrix A we started from suitably so that this would be true. Thus grouping the equivalent matrices R_i in (11) together and choosing C properly, we could suppose that

$$C^{-1}RC = \begin{matrix}[R_1, & R_2, & \ldots] \\ f_1 & f_2 & \end{matrix} \tag{12}$$

where R_j is a R-matrix repeated f_j times in the direct sum. Correspondingly we may suppose that

$$C'AC = \begin{matrix}[A_1, & A_2, & \ldots] \\ f_1 & f_2 & \end{matrix} \tag{13}$$

where, again, A_j are repeated f_j times. Now in (12), R_j is not equivalent to R_k over $\mathbb{Q}$ for $j \neq k$. On the other hand, it could happen that $A_j = A_k$ for $j \neq k$, in (13).

We shall suppose, in the sequel, that R and A are already in the form given on the right hand side of (12) and (13) respectively.

Let us consider the set of linear equations defined by the single matrix equation $RM = MR$. This is a system of $4n^2$ linear equations in $4n^2$ unknowns with roal coeffiecients, namely the elements of R. In order to reduce this to a set a equations with rational coefficients, we shall adopt **12** the following procedure.

Let $\rho_1, \rho_2, \ldots, \rho_p$ be a maximal set of elements r_{kl} of R which are linearly independent over $\mathbb{Q}$. We may then write

$$R = \rho_1 L_1 + \ldots + \rho_p L_p \tag{14}$$

where $L_1, \ldots L_p$ are rational $2n$-rowed square matrices. Denote by $\mathscr{T}$ the abstract algebra generated by $L_1, \ldots, L_p$ over $\mathbb{Q}$ and by $(\mathscr{T})$, the matrix representation by the $L_i's$. In other words, $(\mathscr{T})$ is the algebra consisting of elements T of the form $T = \sum_{1 \leq k_1, \ldots, k_m \leq p} a_{k_1 \ldots k_m} L_{k_1} \ldots L_{k_m} (a_{k_1 \ldots k_m} \in \mathbb{Q})$ and the $2n$-rowed identity E. By definition, $\mathscr{T}$ is uniquely determined by R, since a change of $\rho_1, \ldots, \rho_p$ would merely involve taking instead of $L_1, \ldots L_p$ matrices $T_1, \ldots T_p$ which are rational linear combinations of $L_1, \ldots, L_p$ and vice versa.

Incidentally, we remark that the determination of $L_1, \ldots, L_p$ in (14) is not all that simple as it appears. For, take the the simple 2-rowed R-matrix $\begin{pmatrix} 0 & -1/\sqrt{\gamma} \\ \sqrt{\gamma} & 0 \end{pmatrix}$ with $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and γ begin Euler's constant. It is rather ironical that one does not know whether $\sqrt{\gamma}$ and $1/\sqrt{\gamma}$ are linearly independent over $\mathbb{Q}$.

The relationship between $(\mathfrak{M})$ and $(\mathscr{T})$ is given by

Proposition 3. The algebra $(\mathfrak{M})$ is the commutator algebra of $(\mathscr{T})$. (Definition. *By the* commutator algebra *of* $(\mathscr{T})$*, we mean the set of all* $2n$*-rowed rational square matrices* M *for which* $TM = MT$ *for all* $T \in (\mathscr{T})$*).*

Proof. For each $M \in (\mathfrak{M})$, we have **13**

$$0 = RM - MR = \sum_{j=1}^{p} \rho_j (L_j M - M L_j).$$

But now $\rho_1, \ldots, \rho_p$ being linearly independent over $\mathbb{Q}$ and since $L_j M - M L_j$, $j = 1, 2, \ldots, p$ are rational matrices, we deduce that $L_j M = M L_j$ for $1 \leq j \leq p$. Hence $TM = MT$ for all $T \in (\mathscr{T})$. The converse is trivial, since if M is in the commutator algebra of $(\mathscr{T})$, then M commutes with L_j for $1 \leq j \leq p$ and hence with R by (14). Thus $(\mathfrak{M})$ is precisely commutator algebra of $(\mathscr{T})$. □

Proposition 4. *The algebra* $(\mathscr{T})$ *admits the involution* $T \to T^* = A^{-1} T' A$.

Proof. First of all, we see that for the basis elements L_j, $j = 1, 2, \ldots p$ of $(\mathscr{T})$, we have $L_j^* = -L_j$. For, from $A' = -A$, $S = S'$, we have $R^* = -R$ and further $R^* = (\rho_1 L_1 + \ldots + \rho_p L_p)^* = \rho_1 L_1^* + \ldots + \rho_p L_p^* = -(\rho_1 L_1 + \ldots + \rho_p L_p)$. In other words, we have

$$\rho_1 (L_1 + L_1^*) + \ldots + \rho_p (L_p + L_p^*) = 0.$$

Again, since $L_j + L_j^*$, $1 \leq j \leq p$ are rational and $\rho_1, \ldots, \rho_p$ are linearly independent over $\mathbb{Q}$, we have $L_j^* = -L_j (1 \leq j \leq p)$. And now, for any $T = \sum_{1 \leq k_1, \ldots, k_m \leq p} a_{k_1 \ldots k_m} L_{k_1} \ldots L_{k_m}$, we see that

$$T^* = \sum a_{k_1 \ldots k_m} L_{k_m}^* \ldots L_{k_1}^* = \sum_{1 \leq k_1, \ldots, k_m \leq p} a_{k_1 \ldots k_m} L_{k_m} \ldots L_{k_1} \in (\mathscr{T}).$$

That the mapping $T \to T^*$ is an involution of $(\mathscr{T})$ is quite clear.

14 Let us remark that the involution $T \to T^*$ of $(\mathscr{T})$ is not necessarily a positive involution. The fact that $S = AR$ is symmetric is equivalent to the fact that $(\mathscr{T})$ is closed under an involution $T \to T^*$ such that $L_j^* = -L_j$, $1 \leq j \leq p$. Therefore, the condition that S is positive symmetric is much stronger than $(\mathscr{T})$ admitting the special involution $T \to T^*$.

Since $R = \begin{smallmatrix} [R_1, & R_2, & \ldots] \\ f_1 & f_2 & \end{smallmatrix}$, it is clear that every L_i is of the form as R, in view of the linear independence of $\rho_1, \ldots \rho_p$ over $\mathbb{Q}$. Thus, any $T \in (\mathscr{T})$ is of the form $\begin{smallmatrix} [T_1, & T_2, & \ldots] \\ f_1 & f_2 & \end{smallmatrix}$ with T_j being repeated f_j times in the direct

sum. For fixed j, let us denote by $(\mathscr{T}_j)$ the algebra generated over $\mathbb{Q}$ by such rational matrices T_j and the corresponding abstract algebra by $\mathscr{T}_j$. None of the $\mathscr{T}_j$ can be the null-algebra for then we will have $R_j = 0$, contradicting $R^2 = -E$. □

Remark. For $k \neq 1$, it could happen that $\mathscr{T}_k$ and $\mathscr{T}_1$ are isomorphic. But *there cannot exist a nonsingular rational matrix B independent of* $T = \begin{matrix}[T_1, & T_2, & \ldots] \\ f_1 & f_2 & \end{matrix} \in (\mathscr{T})$ *such that for* $k \neq 1$, $T_k = B^{-1}T_1B$ *for every* $T \in (\mathscr{T})$. For, if such a B were to exist then $R_k = B^{-1}R_1B$ for $k \neq 1$, which is a contradiction.

Each algebra $(\mathscr{T}_j)$ is necessarily irreducible (since, if $(\mathscr{T}_j)$ were reducible, we would have R_j necessarily reducible).

By a *simple algebra*, we mean an irreducible matrix algebra [28]. This definition of a simple algebra can be identified with another of a simple (matrix) algebra as one having no proper two-sided ideals. A *semi-simple algebra* is, by definition, a direct sum of simple algebras. **15**

Proposition 5. *The algebra* $(\mathscr{T})$ *is semi-simple.*

Proof. The algebras $(\mathscr{T}_j)$ are simple and if we could show that $\mathscr{T}$ is the direct sum of the algebras $\mathscr{T}_j$, then our proposition would be proved. For this, it is sufficient to prove that if $T_j \in (\mathscr{T}_j)$, then $T = \begin{matrix}[0 & 0 & , & T_1 & 0] \\ f_1^{,\ldots,} & f_{l-1} & , & f_1^{,\ldots,} & f_p\end{matrix} \in (\mathscr{T})$ for every l with $1 \leq l \leq p$. We might suppose, without loss of generality that $l = 1$. Let now, for $1 \leq j \leq p$, $(\mathfrak{N}_j)$ be the set of $T_j \in (\mathscr{T}_j)$ such that $T = \begin{matrix}[*,\ldots, & *, & T_j, & 0,\ldots, & 0] \\ f_1 & f_{j-1} & f_j & f_{j+1} & f_p\end{matrix}$ is in $(\mathscr{T})$. It is easy to verify that $(\mathfrak{N}_j)$ is a two-sided ideal in $(\mathscr{T}_j)$. Now $(\mathscr{T}_j)$ being simple, we have $(\mathfrak{N}_j) = (\mathscr{T}_j)$ or $(\mathfrak{N}_j)$ is the null-algebra. If $(\mathfrak{N}_1) = (\mathscr{T}_1)$, we are through. Otherwise, let k be the smallest positive integer greater than 1 such that $(\mathfrak{N}_{k-1})$ is the null-algebra and $(\mathfrak{N}_k)$ is the whole of $(\mathscr{T}_k)$. Then necessarily, $2 \leq k \leq p$ for otherwise $(\mathscr{T}_p)$ will be the null-algebra which is not true, as we know. We now claim that if $T = \begin{matrix}[T_1,\ldots, & T_{k-1}, & T_k,\ldots, & 0] \\ f_1 & f_{k-1} & f_k & f_p\end{matrix}$ is in $(\mathscr{T})$, then corresponding to $T_k \in (\mathscr{T}_k)$, T_{k-1} in $(\mathscr{T}_{k-1})$ is uniquely determined. For, if $T = \begin{matrix}[T_1,\ldots, & T_{k-1}, & T_k, & 0,\ldots, & 0] \\ f_1 & f_{k-1} & f_k & f_{k+1} & f_p\end{matrix} \in (\mathscr{T})$ and $M = \begin{matrix}[M_1,\ldots, & M_{k-1}, & T_k, & 0\ldots & 0] \\ f_1 & f_{k-1} & f_k & f_{k+1} & f_p\end{matrix} \in (\mathscr{T})$, then $T_{k-1} - M_{k-1} \in (\mathfrak{N}_{k-1})$ which is the null-algebra, by definition of k. Thus there is a one-one correspondence $T_k \leftrightarrow T_{k-1}$ between $(\mathscr{T}_k)$ **16**

and $(\mathscr{T}_{k-1})$ which is actually an algebra isomorphism. But now $(\mathscr{T}_k)$ and $(\mathscr{T}_{k-1})$ are irreducible, and therefore there exists a constant non-singular rational matrix B such that if $T = \begin{bmatrix} \ldots & T_{k-1}, & T_k, & . \\ & f_{k-1} & f_k & \end{bmatrix} \in (\mathscr{T})$, then $T_{k-1} = B^{-1}T_kB$, which is a contradiction to our Remark on p. 11. Then $(\mathfrak{N}_1) = (\mathscr{T}_1)$ and similarly we can show $(\mathfrak{N}_j) = (\mathscr{T}_j)$ for every j.

By a theorem on algebras, the commutator algebra of a semi-simple matrix algebra is again semi-simple. Thus $(\mathfrak{M})$ which is the commutator-algebra of $(\mathscr{T})$ is semi-simple. (Compare the proof of Theorem 1.4-A, p.717, [28]). We shall however find the structure of $(\mathfrak{M})$ explicitly, as follows.

We may write $R = \begin{bmatrix} R_1, & R_2, \ldots \\ f_1 & f_2 \end{bmatrix}$ as

$$R = \left[R^{(1)}, R^{(2)}, \ldots, \right]$$

and correspondingly $T = \begin{bmatrix} T_1, & T_2 \cdots \\ f_1 & f_2 \end{bmatrix} \in (\mathscr{T})$ as

$$T = [T^{(1)}, T^{(2)}, \ldots,]$$

Again, we decompose $M \in (\mathfrak{M})$ correspondingly as (M_{kl}). From $TM =$
17 MT, it follows

$$T^{(k)}M_{kl} = M_{kl}T^{(l)} \tag{15}$$

where $T^{(k)}$, $T^{(l)}$ run over all elements of $(\mathscr{T}_{j_k})$ and $(\mathscr{T}_{j_l})$ respectively. But now the algebras $(\mathscr{T}_j)$ are irreducible. Therefore applying Schur's lemma, we see that either M_{kl} is the zero matrix or if M_{kl} is a square matrix (different from the zero matrix), then it is necessarily non-singular. Let us suppose now that $j_k \neq j_l$. If M_{kl} is a square matrix different from zero, then it is necessarily a nonsingular (rational) matrix and this contradicts the remark on p. 1. Thus corresponding to the decomposition $\begin{bmatrix} R_1, & R_2 \cdots \\ f_1 & f_2 \end{bmatrix}$ of R, the matrix $M \in (\mathscr{M})$ takes the form $[M_1, M_2, \ldots]$ where $M_k = (M_{pq}^{(k)})$ and from (15),

$$T_kM_{pq}^{(k)} = M_{pq}^{(k)}T_k \tag{16}$$

for every $T_k \in (\mathscr{T}_k)$. Thus $M_{pq}^{(k)}$ belongs to the commutator algebra of $(\mathscr{T}_k)$ which we may denote by $(\mathfrak{L}_k)$. By Schur's lemma again, since

$(\mathscr{T}_k)$ is irreducible, we see from (16) that $M_{pq}^{(k)} = 0$ or it is non-singular. Thus the matrix algebra $(\mathfrak{L}_k)$ is indeed a division-algebra. Conversely, if $M = [M_1, \ldots, M_k, \ldots]$ where $M_k = (M_{pq}^{(k)})$, and $M_{pq}^{(k)} \in (\mathfrak{L}_k)$, then $M \in (\mathfrak{M})$. Thus $(\mathfrak{M})$ is the direct sum $(\mathfrak{M}_1) + (\mathfrak{M}_2) + \ldots$ where $(\mathfrak{M}_k)$ is the complete f_k-rowed matrix algebra over the division algebra $(\mathfrak{L}_k)$. Each $(\mathfrak{M}_k)$ is a simple algebra, since it is the complete matrix algebra **18** over a division algebra. Thus $(\mathfrak{M})$ is semi-simple.

Let us remark that one could prove the fact $(\mathfrak{M})$ is semi-simple also directly by making use of the positive involution in $(\mathfrak{M})$.

In the direct sum decomposition $(\mathfrak{M}) = (\mathfrak{M}_1) + (\mathfrak{M}_2) + \ldots$ above, each $(\mathfrak{M}_k)$ is a complete matrix-algebra over a division-algebra $(\mathfrak{L}_k)$ and $(\mathfrak{M}_k)$ carries a positive involution which, when restricted to $(\mathfrak{L}_k)$ is again a positive involution. Thus, in our study of the commutator algebra of a R-matrix, we are finally reduced to the case of division algebras of finite rank over $\mathbb{Q}$, carrying a positive involution. □

3 Division algebras over $\mathbb{Q}$ with a positive involution

We now consider a division algebra $(\mathfrak{M})$ with a positive involution, realised as the commutator algebra of a simple (matrix) algebra $(\mathscr{T})$. From the theory of algebras, it is known that the commutator algebra of $(\mathfrak{M})$ is precisely $(\mathscr{T})$.

Regarding the subalgebra $(\mathfrak{R}) = (\mathscr{T}) \cap (\mathfrak{M})$, we have

Proposition 6. *The algebra* $(\mathfrak{R})$ *coincides with the centre of* $(\mathscr{T})$ *as also with the centre of* $(\mathfrak{M})$.

Proof. Let $K \in (\mathfrak{R})$. Then, since $K \in (\mathfrak{M})$, K belongs to the centre of **19** $(\mathscr{T})$. Conversely, if L is in the centre of $(\mathscr{T})$, then $L \in (\mathfrak{M})$, by our remark on commutator algebras above and therefore $L \in (\mathfrak{R})$. Again let $K \in (\mathfrak{R})$. Then K is in the centre of $(\mathfrak{M})$, since $K \in (\mathscr{T})$. Conversely, if L belongs to the centre of $(\mathscr{T})$, then $L \in (\mathfrak{M})$ clearly.

Since $(\mathfrak{M})$ is a division algebra, its centre $(\mathfrak{R})$ is a field which is a representation of an algebraic number field $\mathfrak{R}$ of degree h, say, over $\mathbb{Q}$. We denote the conjugates of $\mathfrak{R}$ by $\mathfrak{R}^{(1)}(= \mathfrak{R}), \mathfrak{R}^{(2)}, \ldots, \mathfrak{R}^{(h)}$. For $\alpha \in \mathfrak{R}$,

we denote its conjugates by $\alpha^{(1)} \ldots\ldots, \alpha^{(h)}$, and the 'trace' $\alpha^{(1)} + \ldots + \alpha^{(h)}$ and 'norm' $\alpha^{(1)}, \ldots \alpha^{(h)}$ respectively by $tr_{\Re/\mathbb{Q}}(\alpha)$, $N_{\Re/\mathbb{Q}}(\alpha)$.

The involution $M \to M^*$ of $(\mathfrak{M})$, when restricted to $(\Re)$, gives an automorphism $K \to K^*$ of $\Re$, of order 2. We now distinguish between the following two cases:

(i) for every element κ of $\Re$, $\kappa^* = \kappa$.

(ii) there exists at least one $\kappa_\circ \in \Re$ such that $\kappa_\circ^* \neq \kappa_\circ$.

20 In the case of (i), we say that the *involution is of the first kind* and in the case of (ii), we say it is *of the second kind*.

The positive involution in $(\Re)$ enables us to characterise the field $\Re$ further, as follows. □

Theorem 2. *In the case of positive involutions of the first kind, $\Re$ is totally real. In the case of positive involutions of the second kind, $\Re$ is a totally complex field which is an imaginary quadratic extension of a totally real field $\mathscr{L}$.*

Proof. First, we take the case of a positive involution of the first kind in $\Re$. To $\kappa \in \Re$, there corresponds $K \in (\Re)$. Now $\sigma(KK^*) = \sigma(K^2) > 0$ for every K in $(\Re)$, different from 0. But $(\Re)$ is a multiple of the "regular representation" of $\Re$ over $\mathbb{Q}$ (upto equivalence) and hence $\sigma(K^2) = m.\, tr_{\Re/\mathbb{Q}}(\kappa^2)$ where, m is a positive rational integer. Thus for $\kappa \neq 0$ in $\Re$, we have

$$tr_{\Re/\mathbb{Q}}(\kappa^2) \neq 0 \tag{17}$$

Suppose now $\Re$ is not totally real; in fact, let $\Re^{(1)}$ and $\Re^{(2)}$ be a pair of complex conjugates, without loss of generality. Let $\omega_1, \omega_2, \ldots, \omega_h$ be a basis of $\Re$ over $\mathbb{Q}$. Then we have, for $1 \leq k \leq h$, $\kappa^{(k)} = \sum_{j=1}^{h} x_j \omega_j^{(k)}$ with $x_j \in \mathbb{Q}$. Now $tr_{\Re/\mathscr{Q}}(\kappa^2) = F(x_1, \ldots, x_h)$ is a quadratic form in $x_1, \ldots, x_h$ with coefficients in $\mathbb{Q}$ and it assumes positive (rational) val-
21 ues for rational $x_1, \ldots, x_h$ not all zero. Hence, in the first place F is nondegenerate since if F is degenerate, there exists a rational column $\underline{x}_0 = 0$ where F_1 is the matrix associated with $F(x_1 \ldots x_h)$ and then $\underline{x}_0' F_1 \underline{x}_0 = F(x_1^{(0)}, \ldots x_h^{(0)}) = 0$ for rational $x_1^{(0)}, \ldots x_h^{(0)}$ not all zero. By

continuity, it can be seen that it is, in fact, a positive-definite quadratic form in $x_1, \ldots, x_h$. Since the matrix $(\omega_k^{(j)})(1 \leq k, j \leq h)$ is non-singular and $\mathfrak{R}^{(1)}, \mathfrak{R}^{(2)}$ are complex fields, it is possible to find real numbers $x_1^{(0)}, \ldots, x_h^{(0)}$ such that

$$\omega_1^{(1)} x_1^{(0)} + \ldots + \omega_h^{(1)} x_h^{(0)} = i$$

$$\omega_1^{(2)} x_1^{(0)} + \ldots + \omega_h^{(2)} x_h^{(0)} = -i$$

$$\omega_1^{(j)} x_1^{(0)} + \ldots + \omega_h^{(j)} x_h^{(0)} = 0 \text{ for } 2 < j \leq h.$$

Now $F(x_1^{(0)}, \ldots x_h^{(0)}) = i^2 + (-i)^2 + 0 + \ldots + 0 = -2 < 0$. We can, by continuity of $F(x_1, \ldots, x_h)$ again, find rational numbers $x_1', \ldots, x_h'$ sufficiently close to $x_1^{(0)}, \ldots, x_h^{(0)}$ such that $F(x_1', \ldots, x_h') < 0$, which is a contradiction. Thus $\mathfrak{R}$ is necessarily totally real.

We now take the case of involutions of the second kind. Let $\mathscr{L}$ be the fixed field of the involution, viz. the set of all $\kappa \in \mathfrak{R}$ such that $\kappa^* = \kappa$. Since the involution is of the second kind, there exists $\kappa_0 \in \mathfrak{R}$ such that $\kappa_0 \neq \kappa_0^*$; clearly $\kappa_0 \notin \mathscr{L}$. We now claim that $\rho = \kappa_0 - \kappa_0^* (\neq 0!)$ generates $\mathfrak{R}$ over $\mathscr{L}$. For $\rho = -\rho^*$ and $\rho^2 = \delta \in \mathscr{L}$, $\delta \neq 0$. An arbitrary $\kappa \in \mathfrak{R}$ can be written as $\frac{1}{2}(\kappa + \kappa^*) + \frac{1}{2\rho}(\kappa - \kappa^*) = \lambda + \mu\rho$ (say). Obviously $\lambda, \mu \in \mathscr{L}$ and further,

$$\text{if } \kappa = \lambda + \mu\rho \text{ with } \lambda, \mu \in \mathscr{L}, \text{ then } \kappa^* = \lambda - \mu\rho. \tag{18}$$

(It is trivial that any $\lambda + \mu\rho$ with $\lambda, \mu \in \mathscr{L}$ belongs to $\mathfrak{R}$). Now if $K \in (\mathfrak{R})$ **22**
corresponds to $\kappa \in \mathfrak{R}$, then $\sigma(KK^*) > 0$ for $K \neq 0$ implies that $tr_{\mathfrak{R}/\mathbb{Q}}((\lambda + \mu\rho)(\lambda - \mu\rho)) = tr_{\mathfrak{R}/\mathbb{Q}}(\lambda^2 - \mu^2\delta) > 0$ for all $\lambda, \mu \in \mathscr{L}$ not both zero. (Recall that $\sigma(KK^*) = m.tr_{\mathfrak{R}/\mathbb{Q}}(\kappa\kappa^*)$ for a positive integer m). But we know that $tr_{\mathfrak{R}\mathbb{Q}}(\kappa\kappa^*) = tr_{\mathscr{L}/\mathbb{Q}}(tr_{\mathfrak{R}/\mathscr{L}}(\kappa\kappa^*)) = 2tr_{\mathscr{L}/\mathbb{Q}}(\lambda^2) - 2tr_{\mathscr{L}/\mathbb{Q}}(\mu^2\delta)$. In particular, for $\lambda \neq 0$ in $\mathscr{L}$, $tr_{\mathscr{L}/\mathbb{Q}}(\lambda^2) > 0$ which implies, by the foregoing arguments that $\mathscr{L}$ is totally real. We now claim that δ is necessarily totally negative. For, if one particular conjugate, say $\delta^{(j)} > 0$, then we can find an element ε in $\mathscr{L}$ such that $|\varepsilon^{(j)}|$ is large and $|\varepsilon^{(k)}| \leq 1$ for $k \neq j$ so that $tr_{\mathscr{L}/\mathbb{Q}}(-\varepsilon^2\delta) < 0$ which gives a contradiction. Thus $\mathfrak{R} = \mathscr{L}(\sqrt{\delta})$ i.e. $\mathfrak{R}$ is an imaginary quadratic extension of the totally real field $\mathscr{L}$. □

Remark. In the case of positive involutions of the second kind, the *involution is uniquely determined* by (18), viz. if $\kappa = \lambda + \mu\sqrt{\delta}$ with λ, $\mu \in \mathscr{L}$, then $\kappa^* = \lambda - \mu\sqrt{\delta}$ which is just the complex conjugate of κ. If the involution is not positive, then it is not uniquely determined, in general. Take the biquadratic field generated by $\sqrt{2}$ and $\sqrt{3}$ over $\mathbb{Q}$; we have two distinct involutions, $\sqrt{2} \to -\sqrt{2}$ and $\sqrt{3} \to -\sqrt{3}$.

Having known the structure of the centre $\mathfrak{R}$ of the algebra $\mathfrak{M}$, we wish to remark that the division algebra $\mathfrak{M}$ can be considered as an algebra even over $\mathfrak{R}$, or, in the notation of the theory of algebras, a *central*
23 *algebra*. For, let $\kappa_1, \ldots, \kappa_h$ be a basis of $\mathfrak{R}$ over $\mathbb{Q}$ and let us denote the identity in $\mathfrak{M}$ by γ_1. Then $\kappa_1\gamma_1, \ldots\ldots\ldots, \kappa_h\gamma_1$ are linearly independent over $\mathbb{Q}$. If there exists γ_2 in $\mathfrak{M}$ linearly independent of these h elements, then it is easy to see that $\kappa_1\gamma_1, \ldots \kappa_h\gamma_1, \kappa_1\gamma_2, \ldots, \kappa_h\gamma_2$ are linearly independent over $\mathbb{Q}$. In this way, we can find $\gamma_1, \gamma_2, \ldots \gamma_m$ in $\mathfrak{M}$ such that $\kappa_1\gamma_1, \ldots, \kappa_h\gamma_1, \kappa_1\gamma_2, \ldots, \kappa_h\gamma_2, \ldots, \kappa_h\gamma_m$ form a basis of $\mathfrak{M}$ over $\mathbb{Q}$ and $\gamma_1, \ldots, \gamma_m$ form a basis of $\mathfrak{M}$ over $\mathfrak{R}$. Thus $\mathfrak{M}$ is a central algebra of rank m over $\mathfrak{R}$. It is known from the theory of algebras that $m = s^2$, where s is a rational integer.

In connection with the problem of determining the division algebras over $\mathbb{Q}$ with a positive involution, occurring as the complete commutator algebra of a R-matrix, we shall find, as a first step, all division algebras over $\mathbb{Q}$ carrying a positive involution. In view of our remark above, it clearly suffices to find all central division algebras with a positive involution over a given field of the type mentioned in Theorem 2. Then, given one positive involution therein, we shall obtain all positive involutions in the algebra. We shall also examine the possibility of expressing the given positive involution in the specific form $M \to A^{-1}M'A$ (in the regular representation) with a rational non-singular skew-symmetric matrix A and then getting from one such A, all other principal matrices for the same involution.

First we proceed to determine all central division algebras $\mathscr{V}$ with a positive involution, over a given number field.

24 Let $\mathscr{V}$ be commutative. Then, by Theorem 2, $\mathscr{V}$ is either a totally complex or a totally real number field $\mathfrak{R}$, of degree h, say, over $\mathbb{Q}$. Let $\mathfrak{R}^{(1)}, \ldots, \mathfrak{R}^{(h)}$ be the conjugates of $\mathfrak{R}$ and $\omega_1, \ldots, \omega_h$ be a basis of $\mathfrak{R}$

over $\mathbb{Q}$. We now consider the so-called *regular representation* of $\mathfrak{R}$ over $\mathbb{Q}$ (relative to $\omega_1, \ldots, \omega_h$). For any $\delta \in \mathfrak{R}$, we have $\omega_k \delta = \sum_{j=1}^{h} x_{kj}\omega_j$, $1 \leq k \leq h$, $x_{kj} \in \mathbb{Q}$.

$$\omega_k^{(1)}\delta^{(1)} = \sum_{j=1}^{h} x_{kj}\omega_j^{(1)}, \quad 1 \leq k, \quad 1 \leq h. \tag{19}$$

Denoting the matrices $[\delta^{(1)}, \ldots, \delta^{(h)}]$, $(\omega_k^{(1)})$ and (x_{kj}) by (δ), Ω and D respectively, we rewrite (19) in matrix form as

$$\Omega(\delta) = D\Omega \tag{19}'$$

The mapping $(\delta) \to D$ gives a faithful and irreducible rational representation of $\mathfrak{R}$. If $\omega_1, \ldots, \omega_h$ are replaced by $\omega_1', \ldots, \omega_h'$ where $\begin{pmatrix} \omega_1' \\ \vdots \\ \omega_h' \end{pmatrix} = C \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_h \end{pmatrix}$ where C is rational and nonsingular, then we have the equivalent representation $(\delta) \to CDC^{-1}$. All irreducible representations of $\mathfrak{R}$ are equivalent to the regular representation of $\mathfrak{R}$ and an arbitrary 'non-degenerate' representation of $\mathfrak{R}$ is just a multiple of the same.

The involution $\delta \to \delta^*$ in $\mathfrak{R}$ is, in view of our remark on p. 16 given by

$$\delta^* = \begin{cases} \delta, & \text{if the involution is of the first kind} \\ \overline{\delta}, & \text{if it is of the second kind.} \end{cases}$$

Passing to the transpose conjugate in (19)′, we have

$$(\delta^*)\overline{\Omega}' = \overline{\Omega}' D'$$

But $\Omega(\delta^*) = D^*\Omega$. Thus setting $F^{-1} = \Omega\overline{\Omega}'$, we have **25**

$$D^* = F^{-1}D'F.$$

Now, observing that the involution $*$ commutes with all the isomorphisms of $\mathfrak{R}$ i.e. $\overline{\omega_j^{(k)}} = (\overline{\omega}_j)^{(k)}$, we see that $F^{-1} = (tr_{\mathfrak{R}/\mathbb{Q}}(\omega_i\overline{\omega}_j))$ is a rational matrix but being positive hermitian, is positive symmetric.

The rank of a central (matrix) division algebra $\mathscr{V}$ over its centre is s^2, where s is a rational integer. For $s = 1$, $\mathscr{V}$ itself is an algebraic number field $\mathfrak{R}$ and we have seen in detail, the structure of $\mathfrak{R}$ in order that it might carry a positive involution.

Now suppose $s = 2$. The algebra $\mathscr{V}$ is then a so-called *quaternion algebra* over the centre $\mathfrak{R}$. Any element $\delta \in \mathscr{V}$ is of the form $\delta = x + yi + zj + tk$ where i, j, k satisfy the multiplication table given below:

$$i^2 = a \in \mathfrak{R}, \quad j^2 = b \in \mathfrak{R}, \quad k^2 = -ab, \quad ij = -ji = k,$$
$$jk = -bi = -kjki = -aj = -ik.$$

It can be verified that if $1, i, j, k$ are linearly independent over $\mathbb{Q}$ and satisfy the multiplication table above, then they generate an algebra $\mathscr{V}$ of rank 4, with centre $\mathfrak{R}$.

When is this algebra a division algebra with a positive involution?

Now, in $\mathscr{V}$, we have the mapping

$$\delta = x + yi + zj + tk \to \widetilde{\delta} = x - yi - zj - tk$$

26 and it is easy to check that this is an involution of $\mathscr{V}$. Under the regular representation, $\delta \to D$ where D is given by

$$\begin{pmatrix} 1 \\ i \\ j \\ k \end{pmatrix} (x + yi + zj + tk) = D \begin{pmatrix} 1 \\ i \\ j \\ k \end{pmatrix}$$

$$\text{i.e. } D = \begin{pmatrix} x & y & z & t \\ ay & x & at & z \\ bz & -bt & x & -y \\ -abt & bz & -ay & x \end{pmatrix}$$

Now $\widetilde{D} = \begin{pmatrix} x & -y & -z & -t \\ -ay & x & -at & -z \\ -bz & bt & x & y \\ abt & -bz & ay & x \end{pmatrix}$. Defining $F^{-1} = [1, -a, -b, ab]$ it can be seen that $\widetilde{D} = F^{-1}D'F$. The representation $\delta \to D$ is not a representation over $\mathbb{Q}$, but we can get one by replacing each α in D by its regular representation $\Omega(\alpha)\Omega^{-1}$ over $\mathbb{Q}$.

In order that $\mathscr{V}$ is a division algebra, it is necessary and sufficient that the norm of $\delta \in \mathscr{V}$ over $\mathfrak{R}$ is different from zero, for $\delta \neq 0$. But the norm of $\delta = x + yi + zj + tk$ over $\mathfrak{R}$ is just $x^2 - ay^2 - bz^2 + abt^2$. *Hence the necessary and sufficient condition for $\mathscr{V}$ to be a division algebra is*

that the quadratic form $f(x,y,z,t) = x^2 - ay^2 - bz^2 + abt^2$ *should not represent 0 non-trivially over* $\mathfrak{R}$.

We shall now find conditions under which the involution $\delta \to \widetilde{\delta}$ in $\mathscr{V}$ is a positive involution.

More generally, let us take a central division algebra $\mathfrak{M}$ of rank m **27**
over its centre $\mathfrak{R}$ and let $\delta \to \delta^*$ be an involution in $\mathfrak{M}$, which is identity on $\mathfrak{R}$. We shall now give the "regular representation" of $\mathfrak{M}$ over $\mathfrak{R}$. Let $\gamma_1, \ldots, \gamma_m$ be a basis of $\mathfrak{M}$ over $\mathfrak{R}$ and $\omega_1, \ldots, \omega_h$ be a basis of $\mathfrak{R}$ over $\mathbb{Q}$. Then, for any $\delta = \sum_{j=1}^{m} x_j \gamma_j \in \mathfrak{M}$, we have

$$\begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_m \end{pmatrix} \gamma = D \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_m \end{pmatrix} \tag{20}$$

where $D = (d_{pq})$ is an m-rowed square matrix with elements in $\mathfrak{R}$. For getting a rational representation of $\mathfrak{M}$, we may proceed as follows. Under the regular representation of $\mathfrak{R}$ with respect to the basis $\omega_1, \ldots, \omega_h$, we know that $d_{pq} \to D_{pq} = \Omega[d_{pq}^{(1)}, \ldots, d_{pq}^{(h)}]\Omega^{-1}$ where $\Omega = (\omega_g^{(1)})$, $1 \leq g$, $1 \leq h$. Let us now take as a basis of $\mathfrak{M}$ over $\mathbb{Q}$, the mh elements $\beta_1, \ldots, \beta_{mh}$ defined by $\beta_{k+(l-1)h} = \omega_k \gamma_1$ for $1 \leq k \leq h$, $1 \leq l \leq m$. Then we have for $\delta \in \mathfrak{M}$,

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_{mh} \end{pmatrix} \delta = D_0 \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_{mh} \end{pmatrix} \tag{21}$$

where $D_0 = (D_{pq})(1 \leq p, q \leq m)$ is clearly rational. We can get the relationship between D_0 and D as follows. Suppose, instead of $\beta_1, \ldots, \beta_{mh}$, we take as a basis of $\mathfrak{M}$ the mh elements $\alpha_1, \ldots, \alpha_{mh}$ where $\alpha_{1+(k-1)m} = \omega_k \gamma_1 (1 \leq k \leq h, 1 \leq l \leq m)$ and suppose V is the mh-rowed permutation matrix taking $(l+(k-1)m)^{\frac{th}{\cdots}}$ row to $(k+(l-1)h)^{\frac{th}{\cdots}}$ row; then with respect to the new basis, $\delta \to V^{-1} D_0 V$. It is now easy to verify that **28**

$$V^{-1} D_0 V = (\Omega \times E_m)[D^{(1)}, \ldots, D^{(h)}](\Omega \times E_m)^{-1} \tag{22}$$

where $D^{(1)} = (d_{pq}^{(1)})$ for $1 \leq l \leq h$ and $\Omega \times E_m$ denotes the mh-rowed square matrix $(\omega_j^{(1)} E_m)$, E_m being the m-rowed identity matrix.

Let $\delta = \sum_{j=1}^{m} x_j \gamma_j \in \mathfrak{M}$ and $\delta \to D$, $\delta^* \to D^*$ under (20). Then $\sigma(DD^*) = f(x_1, \ldots, x_m)$ is a quadratic form in $x_1, \ldots x_m$ with coefficients in $\mathfrak{R}$.

Proposition 7. *The involution $\delta \to \delta^*$ in $\mathfrak{M}$ is positive if and only if $\mathfrak{R}$ is totally real and $f(x_1, \ldots, x_m)$ is totally positive-definite (i.e. $f(x_1, \ldots, x_m)$ as well as its conjugates over $\mathbb{Q}$ are positive-definite quadratic forms).*

Proof. By definition, the involution is positive, if, for every $\delta \in \mathfrak{M}$ we have $\sigma(D_0 D_0^*)$ positive for the image D_0 of δ under (21). Now, by (22), $\sigma(D_0 D_0^*) = \sum_{j-1}^{h} \sigma(D^{(j)}(D^*)^{(j)}) = \sum_{j=1}^{h} \sigma(D^{(j)}(D^{(j)})^*)$ (defining $(D^{(j)})^* = (D^*)^{(j)}$). We have thus

$$\sigma(D_0 D_0^*) = tr_{\mathfrak{R}/\mathbb{Q}}(\sigma(DD^*))$$

Thus we should have, in particular, $tr_{\mathfrak{R}/\mathbb{Q}}(\lambda^2) > 0$ for $\lambda \neq 0$ in $\mathfrak{R}$. Therefore $\mathfrak{R}$ should be totally real, using the arguments in the proof of Theorem 2.

By the foregoing, the involution is positive if and only if $tr_{\mathfrak{R}/\mathbb{Q}}(f(x_1,$
29 $\ldots, x_m)) > 0$ for $x_1, \ldots, x_m$ in $\mathfrak{R}$ not all zero. Now, for $u \neq 0$ in $\mathfrak{R}$, we have $f(x_1 u, \ldots, x_m u) = u^2 f(x_1, \ldots, x_m)$. If, for $x_1^{(0)}, \ldots, x_m^{(0)}$ not all zero, some conjugate of $\kappa = f(x_1^{(0)}, \ldots, x_m^{(0)})$ is negative, then, by choosing $u \in \mathfrak{R}$ suitably, we can make $tr_{\mathfrak{R}/\mathbb{Q}}(\kappa u^2) < 0$, which is a contradiction. Moreover, no conjugate of $f(x_1, \ldots, x_m)$ over $\mathbb{Q}$ can be degenerate, for then there will exist $x_1', \ldots, x_m'$ not all zero in $\mathfrak{R}$ such that $f(x_1', \ldots, x_m') = 0$ and $tr_{\mathfrak{R}/\mathbb{Q}}(f(x_1' \ldots, x_m')) = 0$. Thus the conjugates of $f(x_1, \ldots, x_m)$ are all nondegenerate and represent only totally positive numbers in the respective conjugates of $\mathfrak{R}$ which implies that they are positive definite. Our proposition is thus completely proved.

Going back to the quaternion division algebra $\mathscr{V}$ over $\mathfrak{R}$, we deduce that *the involution $\delta \to \widetilde{\delta}$ is positive if and only if $\mathfrak{R}$ is totally real and further, the quaternary form $x^2 - ay^2 - bz^2 + abt^2$ is totally positive-definite; in other words, $-a$, $-b$ should both be totally positive numbers in $\mathfrak{R}$.*

If $-a, -b$ are not both totally positive, then the involution $\delta \to \widetilde{\delta}$ is not positive. We shall, in this case, look for other involutions in $\mathscr{V}$ which might be positive. We shall first find the relationship between any two involutions in $\mathscr{V}$, which have the same effect on $\mathfrak{R}$.

□

Theorem 3 (Albert, [1])**.** *Let $\delta \to \widetilde{\delta}$ and $\delta \to \delta^*$ be two involutions in a central division algebra $\mathfrak{M}$ with centre $\mathfrak{R}$ and let, for $\alpha \in \mathfrak{R}$, $\widetilde{\alpha} = \alpha^*$. Then there exists $\lambda \neq 0$ in $\mathfrak{M}$ such that for $\delta \in \mathfrak{M}$,*

$$\delta^* = \lambda^{-1}\widetilde{\delta}\lambda, \quad \widetilde{\lambda} = \pm\lambda.$$

30

Proof. The mapping $\delta \to (\widetilde{\delta^*})$, being the composite of two involutions, is an automorphism of $\mathfrak{M}$ and further it in identity on $\mathfrak{R}$. By a theorem of T. Skolem [23], every automorphism of a central simple algebra which is identity on its centre, is an inner automorphism of the algebra. Therefore, there exists $\lambda \neq 0$ in $\mathfrak{M}$ such that

$$\begin{aligned} (\widetilde{\delta^*}) &= \lambda\delta\lambda^{-1} \qquad (23)\\ \text{i.e. } \delta^* &= \widetilde{\lambda}^{-1}\widetilde{\delta}\widetilde{\lambda}. \end{aligned}$$

Replacing δ by δ^* in (23), we get

$$\begin{aligned} \widetilde{\delta} &= \lambda\delta^*\lambda^{-1}\\ &= \lambda\widetilde{\lambda}^{-1}\widetilde{\delta}\lambda^{-1}\widetilde{\lambda}. \end{aligned}$$

In other words, $\lambda^{-1}\widetilde{\lambda}$ commutes with all elements of $\mathfrak{M}$ and hence $\widetilde{\lambda} = \kappa\lambda$ for a $\kappa \in \mathfrak{R}$. Further $\lambda = \widetilde{\kappa}\widetilde{\lambda} = \widetilde{\kappa}\kappa\lambda$. Since $\mathfrak{M}$ is a division algebra, $\widetilde{\kappa}\kappa = 1$.

Now, suppose that $\kappa = -1$; then $\widetilde{\lambda} = -\lambda$. If $\kappa \neq -1$, then setting $\gamma = \kappa + 1$, we have $\gamma \neq C$ and $\widetilde{\gamma}\kappa = (\widetilde{\kappa} + 1)\kappa = \gamma$. Further $\widetilde{\lambda\gamma} = \widetilde{\gamma}\kappa\lambda = \gamma\lambda = \lambda\gamma$. Now $\delta^* = \lambda^{-1}\widetilde{\delta}\lambda = (\lambda\gamma)^{-1}\widetilde{\delta}\lambda\gamma$ for $\kappa \neq -1$, we have

$$\delta^* = \lambda_1^{-1}\widetilde{\delta}\lambda_1 \text{ with } \widetilde{\lambda}_1 = -\lambda_1 \text{ or } \widetilde{\lambda}_1 = \lambda_1.$$

Let now $\delta \to \delta^*$ be a positive involution of the first kind in $\mathscr{V}$; then $\mathfrak{R}$ is totally real. We know that the involution $\delta \to \widetilde{\delta}$ in $\mathscr{V}$ is also of the

first kind. Thus, by Theorem 3, there exists $\lambda \neq 0$ in $\mathscr{V}$ with $\widetilde{\lambda} = \pm\lambda$, such that for $\delta \in \mathscr{V}$.

$$\delta^* = \lambda^{-1}\widetilde{\delta}\lambda. \tag{24}$$

31 If $\widetilde{\lambda} = \lambda$, then $\lambda \in \Re$ and then $\delta^* = \widetilde{\delta}$ i.e. *the involution $\delta \to \delta^*$ coincides with the involution $\delta \to \widetilde{\delta}$.*

Let us suppose now that $\widetilde{\lambda} = -\lambda$. We shall construct $\rho \in \mathscr{V}$ such that $\rho^* = -\widetilde{\rho} \neq 0$ i.e. $\lambda^{-1}\widetilde{\rho}\lambda = -\widetilde{\rho}$ which means $\lambda\widetilde{\rho} + \widetilde{\rho}\lambda = 0$. But then applying the involution $\sim$, we have $\rho\lambda + \lambda\rho = 0$. This again gives $(\rho+\widetilde{\rho})\lambda + \lambda(\rho+\widetilde{\rho}) = 0$. But $\rho+\widetilde{\rho} \in \Re$. Therefore $\rho+\widetilde{\rho} = 0$, since $\lambda \neq 0$. The condition $\rho^* = -\widetilde{\rho}$ implies $\widetilde{\rho} = -\rho$. Expressing ρ as $x+yi+zj+tk$, the condition $\widetilde{\rho} = -\rho$ means that $x = 0$. Further since $\widetilde{\lambda} = -\lambda$, $\lambda = pi+qj+rk$ with $p, q, r \in \Re$. Thus to find $\rho \in \mathscr{V}$ such that $\rho^* = -\widetilde{\rho}$, we have only to find numbers y, z, t in $\Re$ satisfying $\lambda\rho+\rho\lambda = 0$, i.e. $apy+bqz-abrt = 0$. But this last equation is a linear equation in three unknowns over the field $\Re$ and therefore admits of infinitely many solutions. Thus, there exists $\rho_0 = y_0 i + z_0 j + t_0 k \in \mathscr{V}$ such that $\rho_0^* = -\widetilde{\rho}_0$ and $\rho_0 \neq 0$.

We now observe that the involutions $\delta \to \widetilde{\delta}$ and $\delta \to \delta^*$ related by (24), with $\widetilde{\lambda} = -\lambda$, cannot both be positive. For, $tr_{\Re/\mathbb{Q}}(\rho_0\rho_0^*) = -tr_{\Re/\mathbb{Q}}(\rho_0\widetilde{\rho}_0)$. In the case when the involution $\delta \to \widetilde{\delta}$ is positive, we thus conclude that no involution $\delta \to \delta^*$ with $\delta^* = \lambda^{-1}\widetilde{\delta}\lambda$ can be positive unless $\widetilde{\lambda} = \lambda$ in which case both the involutions coincide.

Let us suppose that the involution $\delta \to \widetilde{\delta}$ is not positive. Then, in
32 the first place, $f(x, y, z, t)$ cannot be totally positive definite and if the involution $\delta \to \delta^*(= \lambda^{-1}\widetilde{\delta}\lambda$ with $\widetilde{\lambda} = -\lambda)$ is to be positive, then no conjugate of $f(x, y, z, t)$ over $\mathbb{Q}$ can be negative definite either, since for $\lambda \neq 0$ in $\mathbb{Q}$, $h\lambda^2 = h$. $f(\lambda, 0, 0, 0) = tr_{\Re/\mathbb{Q}}(\lambda^2) = tr_{\Re/\mathbb{Q}}(\lambda\lambda^*)$ must be positive. Now, we claim that no conjugate of $f(x, y, z, t)$ can be positive-definite either. For, $tr_{\Re/\mathbb{Q}}(\rho_0\rho_0^* u^2)$ must be positive for all $u \neq 0$ in $\Re$, i.e. $tr_{\Re/\mathbb{Q}}(-f(0, y_0, z_0, t_0)u^2)$ must be positive for all $u \neq 0$ in $\Re$. But, now, if some conjugate of $f(x, y, z, t)$ were positive-definite, we could choose u suitably so that $tr_{\Re/\mathbb{Q}}(-f(0, y_0, z_0, t_0)u^2) < 0$. We know already that no conjugate of $f(x, y, z, t)$ can be negative definite. Thus $f(x, y, z, t)$ and all its conjugates must be indefinite, if the involution $\delta \to \delta^*(= \lambda^{-1}\widetilde{\delta}\lambda$ with $\widetilde{\lambda} = -\lambda)$ were to be positive. We are thus led to □

Proposition 8. *If the quadratic form $f(x,y,z,t) = x^2 - ay^2 - bz^2 + abt^2$ is totally positive-definite, then the only positive involution in $\mathscr{V}$ is the involution $\delta \to \widetilde{\delta}$; otherwise, in order that there might exist positive involutions in $\mathscr{V}$, $f(x,y,z,t)$ should be totally indefinite.*

In the case when the form $x^2 - ay^2 - bz^2 + abt^2$ is totally indefinite, we remark that by means of a linear transformation in x,y,z,t with coefficients in $\mathfrak{R}$, it can be brought to the form $x^2 - a_1y^2 - b_1z^2 + a_1b_1t^2$ where a_1 and $-b_1$ are totally positive. First, we note that the ternary form $\varphi(y,z,t) = -ay^2 - bz^2 + abt^2$ is necessarily totally indefinite (This is because the three numbers $-a^{(j)}, -b^{(j)}, a^{(j)}, b^{(j)}, 1 \leq j \leq h$ cannot all be of the same sign, in view of the fact that $a^{(j)}$ and $b^{(j)}$ are not both negative). **33**
We can find a linear transformation over $\mathfrak{R}$ which takes $\varphi(y,z,t)$ to the form $-\alpha y^2 - bz^2 + \alpha bt^2$ where $-\alpha$ is any totally negative number represented by $\varphi(y,z,t)$ in $\mathfrak{R}$. Again noticing that the binary form $-bz^2 + \alpha bt^2$ is totally indefinite, we can eventually transform $\varphi(y,z,t)$ to the form $-a_1y^2 - b_1z^2 + a_1b_1t^2$ where a_1 and $-b_1$ are totally positive. Thus we could suppose that the totally indefinite form $x^2 - ay^2 - bz^2 + abt^2$ has already the property that $a, -b$ are totally positive.

For $\alpha \in \mathfrak{R}$, $\alpha > 0$ means α is totally positive. Now since $a > 0$, the element $i = \sqrt{a}$ generates in $\mathscr{V}$, a real field $\mathfrak{R}$ (i). Any $\delta = x + yi + zj + tk$ can be written as $\xi + \eta j$ with $\xi = x + yi$ and $\eta = z + ti$. For $\alpha = a + bi$ in $\mathfrak{R}(i)$, we denote $\overline{\alpha} = a - bi$. Then we have $j\xi = \overline{\xi}j$. Then we obtain a representation of $\mathscr{V}$ (as a vector-space over $\mathfrak{R}$ (i)) given by $\delta = \xi + \eta j \to D_1 = \begin{pmatrix} \xi & \eta \\ b\overline{\eta} & \overline{\xi} \end{pmatrix}$;

$$\begin{pmatrix} 1 \\ j \end{pmatrix} \delta = D_1 \begin{pmatrix} 1 \\ j \end{pmatrix} \tag{25}$$

Now

$$\overline{D}_1 = \begin{pmatrix} \overline{\xi} & \overline{\eta} \\ b\eta & \xi \end{pmatrix} = \mathscr{F} D_1 \mathscr{F}^{-1} \tag{26}$$

where $\mathscr{F} = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$ corresponds to $\delta = j$ under (25). Further

$$\widetilde{D}_1 = \begin{pmatrix} \xi & -\eta \\ -b\overline{\eta} & \xi \end{pmatrix} = \mathrm{J} D_1' \mathrm{J}^{-1} \tag{27}$$

where $\widetilde{D}_1$ corresponds under (25) to $\widetilde{\delta} = x - yi - zj - tk = \overline{\xi} - \eta j$ and **34**

$\mathsf{J} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. The regular representation $\delta \to D$ of $\mathscr{V}$ may be seen to be equivalent to the representation $\delta \to \left(\begin{smallmatrix} D_1 & 0 \\ 0 & \overline{D}_1 \end{smallmatrix}\right)$ as below, viz.

$$D = W\Omega_2 \left(\begin{smallmatrix} D_1 & 0 \\ 0 & \overline{D}_1 \end{smallmatrix}\right) \Omega_2^{-1} W^{-1} \tag{28}$$

where $\Omega_2 = \left(\begin{smallmatrix} E_2 & E_2 \\ iE_2 & -iE_2 \end{smallmatrix}\right)$, E_2 is the 2-rowed identity and W is a permutation matrix.

Let $\delta \to \delta^* = \lambda_1^{-1}\widetilde{\delta}\lambda_1$ with $\widetilde{\lambda_1} = -\lambda_1$ be an involution in $\mathscr{V}$ and let $\delta^* \to D_1^*$, $\widetilde{\delta} \to \widetilde{D}_1$ and $\lambda_1 \to L_1$ under (25). Now $D_1^* = L_1^{-1}\widetilde{D}_1 L_1$ where $L_1 = \left(\begin{smallmatrix} \mu & \gamma \\ \mathfrak{b}\overline{\gamma} & \overline{\mu} \end{smallmatrix}\right) = -\widetilde{L}_1 = -\mathsf{J}L_1'\mathsf{J}^{-1}$, by (27). Thus setting $F_1 = \mathsf{J}^{-1}L_1$, we see F_1 is real symmetric which is equivalent to saying that $\mu = -\overline{\mu}$. Further

$$D_1^* = F_1^{-1}D_1'F_1 \tag{29}$$

Now $\sigma(DD^*) = 2\sigma(D_1D_1^*)$, in view of (28) and (26). Hence, for the involution $\delta \to \delta^*$ to be positive, the quadratic form $\sigma(D_1D_1^*)$ should be totally positive-definite over $\mathfrak{R}$. This again implies, by (29), that $\sigma(D_1F_1^{-1}D_1'F_1)$ should be totally positive. A necessary and sufficient condition for this is given by

Lemma 1. *Let $X = (x_{kl})$, $1 \le k \le g$, $1 \le l \le h$, be a real matrix and let P, Q be real square matrices of h and g rows respectively. Then the quadratic form $\sigma(XPX'Q)$ in x_{kl} is positive-definite if and only if P and Q are both positive-definite or both negative-definite.*

35 *Proof.* There exist real non-singular matrices C and B such that $BPB' = [p_1, \ldots, p_h]$ and $C'QC = [q_1, \ldots, q_g]$. Replacing X by CXB, we can suppose that already P and Q are in the diagonal form. Now $\sigma(XPX'Q) = \sum_{k=1}^{g}\sum_{l=1}^{h} p_l q_k x_{kl}^2$ is positive-definite if and only if $p_l q_k$ are all positive. Thus either $p_1, \ldots, p_h, q_1, \ldots, q_g$ are all positive or all negative. In other words, the necessary and sufficient condition is that P, Q should be both positive-definite or both negative-definite.

The passage from $\xi(= x + yi)$, $\eta(= z + ti)$, $\overline{\xi}$, $b\overline{\eta}$ to x, y, z, t is a nonsingular real linear transformation and we can thus look upon the elements of D_1 as independent variables. Thus taking D_1 for X in lemma

1, the criterion for $\sigma(D_1F_1^{-1}D_1'F_1)$ to be totally positive is that each conjugate of F_1 is either positive-definite or negative-definite. Now we can find $\kappa \in \Re$ such that the conjugates of κ have prescribed signs and if we choose $\kappa\lambda_1$ instead of λ_1, then we get κF_1 instead of F_1. Thus, without changing the $*$ involution, we might require that $F_1 = \begin{pmatrix} -b\overline{\gamma} & -\overline{\mu} \\ \mu & \gamma \end{pmatrix}$ is totally positive-definite. Now $\mu = -\overline{\mu}$ and therefore $\mu = pi$ with $p \in \Re$ and let $\gamma = q + ri$. The conditions for F_1 to be totally positive are

$$\gamma > 0, \quad -b\overline{\gamma} > 0, \quad \mu\overline{\mu} - b\gamma\overline{\gamma} > 0$$

But $-b > 0$ and therefore, these may be rewritten as

$$\gamma > 0, \quad \overline{\gamma} > 0, \quad \gamma + \overline{\gamma} = 2q > 0, \quad -p^2a - b(q^2 - ar^2) > 0$$

It is easy to check that all these conditions can be compressed as

$$q > 0, \quad -b(q^2 - ar^2) > ap^2 \tag{30}$$

It is possible to find p, q, r in $\Re$ satisfying (30) (for example, take $q = 1$, **36**
$p = r = 0$) and therefore, the existence in $\mathscr{V}$ of positive involutions $\delta \to \delta^*(= \lambda_1^{-1}\widetilde{\delta}\lambda_1)$ with $\widetilde{\lambda}_1 = -\lambda_1$ is assured.

Let now $\delta \to \lambda^{-1}\widetilde{\delta}\lambda$ with $\widetilde{\lambda} = -\lambda \in \mathscr{V}$ be another positive involution (of the first kind). Setting $\rho = \lambda_1^{-1}\lambda$, we have $\rho^{-1}\delta^*\rho = \lambda^{-1}\widetilde{\delta}\lambda$. Now, $\rho^* = \lambda^*(\lambda_1^*)^{-1} = (\lambda_1^{-1}\widetilde{\lambda}\lambda_1)(\lambda_1^{-1}\widetilde{\lambda}_1\lambda_1)^{-1} = \rho$. Conversely, if $\rho = \rho^*$, then $\lambda = \lambda_1\rho$ satisfies $\widetilde{\lambda} = -\lambda$. Thus all such involutions $\delta \to \lambda^{-1}\widetilde{\delta}\lambda$ are connected with $\delta \to \delta^*$ by $\lambda^{-1}\widetilde{\delta}\lambda = \rho^{-1}\delta^*\rho$ for a $\rho \in \mathscr{V}$ satisfying $\rho^* = \rho$.

Suppose $\delta \to \lambda_k^{-1}\widetilde{\delta}\lambda_k$, $k = 1, 2$ are two positive involutions of $\mathscr{V}$, with $\widetilde{\lambda}_k = -\lambda_k$. If $\lambda_k \to L_k$ under 25, then $L_2 = L_1R_1$ where R_1 corresponds to $\rho = \lambda_1^{-1}\lambda_2$. Since $\rho^* = \rho$ by the foregoing, we have $R_1^* = R_1$. Then $F_k = \mathsf{J}^{-1}L_k (k = 1, 2)$ should be totally positive. Further $F_2 = F_1R_1$. Conversely, given $R_1 = R_1^*$ such that $F_2 = F_1R_1$ is totally positive, then the element $\lambda_2 \in \mathscr{V}$ corresponding to $L_2 = L_1R_1$ under (25), given a positive involution $\delta \to_z^{-1} \widetilde{\delta}\lambda_2$ in $\mathscr{V}$. □

Lemma 2. *If F is a real m-rowed positive-definite matrix and R is a real matrix such that FR is symmetric, then FR is positive-definite if and only if all the eigenvalues of R are positive.*

Proof. Since F is positive-definite and $FR = R'F'$, we can find real non-singular C such that $F = C'C$ and $FR = C'BC$ with $B = [b_1, \ldots, b_m]$.
37 Then $C'BC = C'CR$ i.e. $B = CRC^{-1}$. Thus the eigenvalues of B and R are the same. Our lemma easily follows.

Choosing the rational representation $\delta \to D_0$ given by (21), we may conclude as follows. *If $D_0 \to D_0^*$ is a positive involution of the first kind in $\mathscr{V}$, then all other positive involutions can be obtained in the form $D_0 \to R_0^{-1}D_0^*R_0$ where $R_0 = R_0^*$ in $\mathscr{V}$ and further all the eigen-values of R_0 are positive. The quadratic form $x^2 - ay^2 - bz^2 + abt^2$ is either totally definite or totally indefinite over $\mathfrak{R}$.*

From (29) and (28), it can be verified that

$$D^* = F^{-1}D'F \tag{31}$$

where $F = W'^{-1}\Omega'^{-1}1_2\begin{pmatrix} F_1 & 0 \\ 0 & \overline{F}_1 \end{pmatrix}\Omega_2^{-1}W^{-1}$. Now

$$F^{-1} = W\Omega_2\begin{pmatrix} F_1^{-1} & 0 \\ 0 & \overline{F}_1^{-1} \end{pmatrix}\Omega_2'W' = W\Omega_2\begin{pmatrix} L_1^{-1} & 0 \\ 0 & \overline{L}_1^{-1} \end{pmatrix}(W\Omega_2)^{-1}W\Omega_2 \times \begin{pmatrix} \mathsf{J} & 0 \\ 0 & \mathsf{J} \end{pmatrix}(W\Omega_2)^{-1}W\Omega_2\Omega_2'W'.$$

Further since $W\Omega_2\begin{pmatrix} L_1^{-1} & 0 \\ 0 & \overline{L}_1^{-1} \end{pmatrix}\Omega_2^{-1}{}_W{}^{-1}$ corresponds to λ_1^{-1} under the regular representation of $\mathscr{V}$, it is a matrix with elements in $\mathfrak{R}$; moreover it is easy to verify that the matrices $W\Omega_2\begin{pmatrix} \mathsf{J} & 0 \\ 0 & \mathsf{J} \end{pmatrix}(W\Omega_2)^{-1}$ and $W\Omega_2\Omega_2'W'$ have again their elements in $\mathfrak{R}$. Thus F^{-1} has elements in $\mathfrak{R}$ and moreover being *a* transform of the totally positive matrix $\begin{pmatrix} F_1^{-1} & 0 \\ 0 & \overline{F}_1^{-1} \end{pmatrix}$ is itself
38 totally positive over $\mathfrak{R}$. Going to the rational representation $\delta \to D_0$ again, we have, from (31), that

$$D_0^* = F_0^{-1}D_0'F_0 \tag{32}$$

where F_0 is a rational positive symmetric matrix. The relation (32) is analogous to what we obtained on p. 25 for the case of fields, in terms of the regular representation over $\mathbb{Q}$.

An important theorem due to Albert (p.161, [1]) says that any division algebra over $\mathbb{Q}$ admitting an involution of the first kind is either an

algebraic number field $\mathfrak{R}$ or a quaternion division algebra over $\mathfrak{R}$. We have discussed precisely for these two cases, all the involutions of the first kind. We may now proceed to study division algebras carrying involutions of the second kind. Such algebras, again, have been studied by Albert [1].

We have, in this connection, to deal with an important class of algebras called *cyclic algebras* first introduced by L.E. Dickson in 1906. □

4 Cyclic algebras

39

Let $\mathfrak{Z}$ be a cyclic extension of degree $s(>1)$ over an algebraic number field $\mathfrak{R}$ of degree h over $\mathbb{Q}$. Let $\tau, \tau^2, \ldots \tau^{s-1}$, τ^s (=identity) be the distinct automorphisms of $\mathfrak{Z}$ over $\mathfrak{R}$. For $\eta \in \mathfrak{Z}$, we denote by $\eta^{(r)}$, the effect of τ^r on η; particular, $\eta^{(s)} = \eta = \eta^{(0)}$.

Let $\mathfrak{M}$ be the set of elements $\delta = \xi_0 + \xi_1 j + \ldots + \xi_{x-1} j^{s-1}$ where $\xi_0, \xi_1, \ldots, \xi_{x-1}$ are in $\mathfrak{Z}$ and j satisfies

$$j\xi = \xi^{(1)} j \tag{33}$$

for $\xi \in \mathfrak{Z}$. By iteration, we get from (33) **40**

$$j^k \xi^{(1)} = \xi^{(k+l)} j^k.$$

This relation may be seen to be valid for all rational integers $k \geq 0$ and l, defining $j^0 = 1$. In particular,

$$j^s \xi = \xi^{(s)} j^s = \xi j^s.$$

We now stipulate that $1, j, j^2, \cdot, j^{s-1}$ are linearly independent over $\mathfrak{Z}$ and

$$j^s = b \tag{34}$$

for some $b(\neq 0) \in \mathfrak{R}$. Under conditions (33) and (34), it can be verified that $\mathfrak{M}$ is an algebra of rank s^2 over its centre $\mathfrak{R}$. A central algebra $\mathfrak{M}$ over $\mathfrak{R}$, constructed as above with an auxiliary cyclic extension $\mathfrak{Z}$ of $\mathfrak{R}$ is called a *cyclic algebra*. The field $\mathfrak{Z}$ is called a *splitting field* for $\mathfrak{M}$. The quaternion algebra is a special case of a cyclic algebra, when $s = 2$.

It is known that every cyclic algebra is a simple algebra. Conversely, by a theorem of Brauer-Hasse-Noether [7], every simple algebra over $\mathbb{Q}$ can be realised as a cyclic algebra over its centre.

For $\delta = \xi_0 + \xi_1 j + \ldots + \xi_{s-1} j^{s-1} \in \mathfrak{M}$, we have the representation $\delta \to D$ of $\mathfrak{M}$ in $\mathfrak{Z}$ given by

$$\begin{pmatrix} 1 \\ j \\ \cdot \\ j^{s-1} \end{pmatrix} \delta = D \begin{pmatrix} 1 \\ j \\ \cdot \\ j^{s-1} \end{pmatrix}$$

where

$$D = \begin{pmatrix} \xi_0 & \xi_1 \ldots & \xi_{s-1} \\ b\xi_{s-1}^{(1)} & \xi_0^{(1)} \ldots & \xi_{s-2}^{(1)} \\ \cdot & \cdot & \cdot \\ b\xi_1^{(s-1)} & b\xi_2^{(s-1)} \ldots & \xi_0^{(s-1)} \end{pmatrix} \tag{35}$$

41 Let us observe that all the terms below the diagonal of D involve b. The regular representation of $\mathfrak{M}$ over $\mathfrak{R}$ is given by

$$\delta \to (\Omega \times E_s)[D^{(1)}, \ldots D^{(s)}](\Omega \times E_s)^{-1}$$

where $\Omega = (\gamma_k^{(1)})$, with $\gamma_1 \ldots \gamma_s$ being a basis of $\mathfrak{Z}$ over $\mathfrak{R}$ and for $D = (d_{pq})$, $D^{(i)} = (d_{pq}^{(i)})$.

The algebra $\mathfrak{M}$ is a division algebra if and only if $|D| \neq 0$ for every $\delta \neq 0$ in $\mathfrak{M}$. For, we know $\mathfrak{M}$ is a simple algebra containing 1 and the condition $|D| \neq 0$ for $\delta \neq 0$ would imply that $\mathfrak{M}$ is free from divisors of zero and therefore, the ideal generated by any $\delta \neq 0$ would be the whole of $\mathfrak{M}$. Conversely, if $\mathfrak{M}$ is a division algebra and $\delta \neq 0$ in $\mathfrak{M}$, it is trivial to see that $|D| \neq 0$.

Writing every $\xi_k \in \mathfrak{Z}$ as $\sum_{l=1}^{s} x_{kl}\gamma_l$, we see that corresponding to $\delta = \sum_{k=0}^{s-1} \xi_k j^k$, $|D|$ is a homogeneous form $f(\ldots, x_{kl}, \ldots)$ of degree s in the variables x_{kl}, with coefficients in $\mathfrak{R}$. The necessary and sufficient condition for $\mathfrak{M}$ to be a division algebra may thus be reformulated as **42** follows, viz. the form $f(\ldots x_{kl}, \ldots)$ should not represent 0 nontrivially over $\mathfrak{R}$.

In the case of the quaternion algebra $\mathscr{V}$ over $\mathfrak{R}(s = 2)$, for $\delta = \xi + \eta j$, $\xi = x + yi, \eta = z + ti$, we have $|D| = \xi\overline{\xi} - b\eta\overline{\eta} = f(x, y, z, t) = x^2 - ay^2 - bz^2 + abt^2$. We know that $\mathscr{V}$ is a division algebra if and only if

$f(x, y, z, t)$ does not represent zero nontrivially in $\mathfrak{R}$. Clearly, for $\eta = 0$, $|D| = x^2 - ay^2 \neq 0$, since $\underline{a}$ is not a square in $\mathfrak{R}$. We may then suppose that, for given $\delta = \xi + \eta j$ in $\mathscr{V}$ $\eta \neq 0$. The condition that $|D| = 0$ is equivalent to the fact that $\underline{b}$ is the norm of an element $\xi\eta^{-1}$ in $\mathfrak{R}(i)$ over $\mathfrak{R}$. Thus the quaternion algebra $\mathscr{V}$ is a division algebra if and only if $\underline{b}$ is not the norm of any element of $\mathfrak{R}(i)$. In the case $s > 2$, we shall find conditions analogous to this, which shall be *sufficient* for the cyclic algebra $\mathfrak{M}$ to be a division algebra.

Theorem 4 (Wedderburn, [24])**.** *Let $\mathfrak{M}$ be a cyclic algebra constructed as above with $1, j, \ldots, j^{s-1}$ as basis over the splitting field $\mathfrak{Z}$ and let $j^s = b$ belong to the centre $\mathfrak{R}$. If for every integer r satisfying $0 < r \leq s-1$, b^r is not the norm of an element ξ of $\mathfrak{Z}$ over $\mathfrak{R}$ then $\mathfrak{M}$ is a division algebra.*

Proof. Let $\delta = \xi_0 + \xi_1 j + \ldots + \xi_k j^k$ where $0 \leq k \leq s-1$, be an arbitrary element of $\mathfrak{M}$. If $k = 0$ and $\delta \neq 0$, then, trivially, δ has an inverse. Let then $k > 0$ and let us suppose $\xi_k \neq 0$. We may, in fact, assume that $\xi_k = 1$, without loss of generality.

We shall first find $\eta_0, \eta_1, \ldots, \eta_{s-k} \in \mathfrak{Z}$ such that $(\eta_0 + \eta_1 j + \ldots + \eta_{s-k} j^{s-k})(\xi_0 + \xi_1 j + \ldots + j^k)$ is of the form $\rho_0 + \rho_1 j + \ldots + \rho_{k-1} j^{k-1}$ and is different from 0. By iteration of this process, we can eventually obtain an inverse for δ, under the hypotheses of the theorem. Now, $(\eta_0 + \eta_1 j + \ldots + \eta_{s-k} j^k)\delta = \rho_0 + \rho_1 j + \ldots + \rho_{s-1} j^{s-1}$ where

$$
\begin{aligned}
\rho_0 &= \eta_0\xi_0 + \eta_{s-k} b \\
\rho_1 &= \eta_0\xi_1 + \eta_1\xi_0^{(1)} \\
\rho_{k-1} &= \eta_0\xi_{k-1} + \eta_1\xi_{k-2}^{(1)} + \eta_2\xi_{k-3}^{(2)} + \cdots + \eta_{k-1}\xi_0^{(k-1)} \\
\rho_k &= \eta_0 + \eta_1\xi_{k-1}^{(1)} + \cdots + \eta_k\xi_0^{(k)} \\
\rho_{k+1} &= \eta_1 + \eta_2\xi_{k-1}^{(1)} + \cdots \\
&\cdots\cdots\cdots\cdots \\
\rho_{s-1} &= \eta_{s-k-1} + \eta_{s-k}\xi_{k-1}^{(s-k)}
\end{aligned}
$$

Taking $\eta_{s-k} = 1$, we can find $\eta_{s-k-1}, \eta_{s-k-2}, \ldots, \eta_0$ inductively such that $\rho_{s-1} = 0, \rho_{s-2} = 0, \ldots, \rho_k = 0$.

If, now, it turns out that $\rho_0 = \rho_1 = \cdots = \rho_{k-1} = 0$, we shall see that we arrive at a contradiction to the hypotheses.

Replacing j by j_0 where, analogous to (33) and (34), j_0 satisfies

$$j_0\xi = \xi^{(1)} j_0 \text{ for } \xi \in \mathfrak{Z}$$
$$1, j_0 \cdots j_0^{s-1} \text{ are linearly independent over } \mathfrak{Z}, \text{ and}$$
$$j_0^s = x \text{ (an indeterminate)},$$

43 we can verify easily that

$$(\eta_0 + \eta_1 j_0 + \cdots + j_0^{s-k})(\xi_0 + \xi_1 j_0 + \cdots + j_0^k) = \eta_0\xi_0 + j_0^s = x - b. \quad (36)$$

Now, for any $\mu = \mu_0 + \mu_1 j_0 + \cdots + \mu_{s-1} j_0^{s-1}$ with $\mu_0, \mu_1, \ldots, \mu_{s-1}$ in $\mathfrak{Z}$, we have

$$\begin{pmatrix} 1 \\ j_0 \\ \vdots \\ j_0^{s-1} \end{pmatrix} \mu = M \begin{pmatrix} 1 \\ j_0 \\ \vdots \\ j_0^{s-1} \end{pmatrix} \quad (37)$$

where $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, C is a k-rowed square matrix with x on the diagonal and the factor $\underline{x}$ only up to the first power below and zeros above, B is a $(s-k)$-rowed square matrix with 1 on the diagonal and zeros above and further the matrices A, B, D are free from x. Let M_1, M_2 correspond respectively to $\eta_0 + \eta_1 j_0 + \cdots + j_0^{s-k}$ and $\xi_0 + \xi_1 j_0 + \cdots + j_0^k$ under (37). Further noting that

$$\begin{pmatrix} 1 \\ j_0 \\ \vdots \\ j_0^{s-1} \end{pmatrix} (x - b) = (x - b) E_s \begin{pmatrix} 1 \\ j_0 \\ \vdots \\ j_0^{s-1} \end{pmatrix}$$

where E_s is the s-rowed identity matrix, we have, from (36), (37) by taking determinants, that

$$|M_1||M_2| = |(x - b)E| = (x - b)^s.$$

But, by using Laplace's expansion of the determinant of M_2 along k-rowed minors of the first k columns of M_2, we observe that

$$|M_2| = (-1)^{s-k} x^k + \cdots + N(\xi_0)$$

where $N(\xi_0)$ is the norm of ξ_0 over $\mathfrak{R}$. Since $|M_2|$ divides the polyno-
44 mial $(x-b)^s$, it follows that it is necessarily equal to $(-1)^{s-k}(x-b)^k$. Comparing the constant terms, we have

$$N(\xi_0) = (-b)^k(-1)^{s-k}$$

i.e.
$$b^k = N(-\xi_0)$$

which is a contradiction to the hypothesis that no $b^r (0 < r < s)$ is the norm of an element of $\mathfrak{Z}$. Our theorem is therefore proved. □

Remark 1. In the hypotheses of Theorem 4, it is sufficient to require that *for divisors t* of *s* satisfying $1 \leq t < s$, b^r *shall not be the norm of any element of* $\mathfrak{Z}$ *over* $\mathfrak{R}$. For, let $0 < r < s$ and $t = g \cdot c \cdot d$ of r and s. Further, let $b^r = N(\xi)$ for $\xi \in \mathfrak{Z}$. Now there exist rational integers p, q such that $pr + qs = t$. Then $b^t = N(\xi^p b^q)$. In particular, if s is a prime, then all these $(s-1)$ conditions reduce to the single condition that $\underline{b}$ should not be the norm of an element ξ in $\mathfrak{Z}$. In this case, $\mathfrak{M}$ is a division algebra. Conversely, as we shall see presently, if $\mathfrak{M}$ is a cyclic division algebra over $\mathfrak{Z}$ with s, a prime, then necessarily b cannot be the norm of any element of $\mathfrak{Z}$ over $\mathfrak{R}$. It has been shown by Hasse [9] that the conditions on b in Theorem 4 are also *necessary* for $\mathfrak{M}$ to be a division algebra. The proof by Hasse involves the use of 'factor systems' in the theory of algebras. We give, in simple cases, a proof of the necessity of Wedderburn's conditions.

Proposition 9. *With the notation of Theorem 4, let for a divisor r of s,* $b^r = N(\xi)$ *for* $\xi \in \mathfrak{Z}$ *and let r and* $\frac{s}{r}$ *be coprime. Then* $\mathfrak{M}$ *cannot be a division algebra.*

Proof. It is sufficient to show that $\mathfrak{M}$ contains divisors of zero, under the **45** given conditions.

Let $s_1 = \frac{s}{r}$ and let $\mathfrak{Z}_{s_1}$ be the fixed field of the group of the automorphisms $1, \sigma^{s_1}, \ldots, \sigma^{(r-1)s_1}$ of $\mathfrak{Z}$ over $\mathfrak{R}$. Then the set $\mathfrak{M}_{s1}$ of elements of the form $\delta = \eta_0 + \eta_1 j^r + \eta_2 j^{2r} + \cdots + \eta_{s_1} j_{-1}^{(s_1-1)r}$ with $\eta_i \in \mathfrak{Z}_{s_1}$ is again an algebra. Now $\mathfrak{M}_{s_1} \subset \mathfrak{M}$ and we shall show that $\mathfrak{M}_{s_1}$ contains divisors of zero.

The element $\alpha = \xi\xi^{s_1} \cdots \xi^{(rs_1-r)}$ lies in ξ_{s_1} and further b^r is the norm of α in ξ_{s_1} over $\mathfrak{R}$. Moreover if $j_0 = j^{r^2}\alpha^{-1}$, then $1, j_0, \ldots, j_0^{s_1-1}$ is a basis of $\mathfrak{M}_{s_1}$ over $\mathfrak{Z}_{s_1}$ and j_0 satisfies a minimum polynomial equation of degree s_1. Now

$$j_0^{s_1} = b^r(N_{\mathfrak{Z}_{s_1/\mathfrak{R}}}(\alpha))^{-1} = 1$$

This gives us a factorization of 0 in $\mathfrak{M}_{s_1}$, viz.

$$0 = (j_0 - 1)(j_0^{s_1-1} + j_0^{s_1-2} + \cdots + 1)$$

and neither of the factors can be zero, since the minimum polynomial of j_0 is of degree s_1. □

Corollary . *If s is a product of distinct primes, then the conditions of Wedderburn in Theorem 4 are also necessary for $\mathfrak{M}$ to be a division algebra.*

5 Division algebras over $\mathbb{Q}$ with involutions of the second kind

Let $\mathscr{V}$ be a division algebra over $\mathbb{Q}$. Then by a theorem due to Brauer-
46 Hasse-Noether, it is known that $\mathscr{V}$ is a cyclic algebra over its centre $\mathfrak{R}$, with a certain cyclic extension over $\mathfrak{R}$ as splitting field.

Conditions necessary and sufficient for $\mathscr{V}$ to have an involution of the second kind have been given by Albert [1]. First, let $\delta \to \widetilde{\delta}$ be such an involution in $\mathscr{V}$. If $\mathscr{L}$ is the fixed field of the involution contained in the centre $\mathfrak{R}$ of $\mathscr{V}$, then $\mathfrak{R} = \mathscr{L}(c)$ is a quadratic extension over $\mathscr{L}$, with a suitable c in $\mathfrak{R}$ satisfying $\widetilde{c} = -c$. In this case, Albert has shown (Chap X, [1]) that one can find a cyclic extension $\xi_0 = \mathscr{L}(\varsigma)$ of degree $\underline{s}$ over $\mathscr{L}$ such that

i) the involution is identity on $\mathfrak{Z}_0$, and

ii) the algebra $\mathscr{V}$ is a cyclic algebra having for its

splitting field the field $\mathfrak{Z} = \mathfrak{Z}_0(c) = \mathscr{L}(c, \varsigma)$ which is abelian of degree $2s$ over $\mathscr{L}$.

Following our earlier notation, let 1, $j, j^2, \ldots, j^{s-1}$ generate $\mathscr{V}$ over $\mathfrak{Z}$ and let $j^2 = b \in \mathfrak{R}$. Now we claim that $\widetilde{jj}$ commutes with all elements of $\mathfrak{Z}$. For, first of all, any $\xi \in \mathfrak{Z}$ is of the form $\xi = \eta_0 + \eta_1 c$ with $\eta_0, \eta_1 \in \mathfrak{K}_0$ and $\widetilde{\xi} = \eta_0 - \eta_1 c$. Hence the mapping $\xi \to \widetilde{\xi}$ is an automorphism of $\mathfrak{Z}$. Denote by σ the generating automorphism of $\mathfrak{Z}$ over $\mathfrak{R}$ and by $\eta^{(1)}$, the effect of σ^1 on $\eta \in \mathfrak{Z}$. Using the fact that $\mathfrak{Z}$ is abelian over $\mathscr{L}$, we have, for $\xi = \eta_0 + \eta_1 c$ (with $\eta_0, \eta_1 \in \mathfrak{K}_0$),

$$\widetilde{\xi^{(l)}} = (\eta_0^{(l)} \widetilde{+ \eta_1^{(l)} c}) = \eta_0^{(l)} - \eta_1^{(l)} \cdot c = (\widetilde{\xi})^{(1)} \tag{38}$$

Now, for $\eta \in \mathfrak{Z}$, we have

$$\tilde{\eta}\tilde{j} = \widetilde{j\eta} = \widetilde{\eta^{(1)} j} = \tilde{j}\widetilde{\eta^{(1)}} = \tilde{j}(\tilde{\eta})^{(1)} \tag{39}$$

and therefore, for $\xi \in \mathfrak{Z}$, we obtain **47**

$$\tilde{j}j\xi = \tilde{j}\xi^{(1)} j = \xi \tilde{j} j$$

using (39) with $\tilde{\eta} = \xi$. Now $\mathfrak{Z}$ is a maximal commutative system in $\mathscr{V}$ and it follows immediately that

$$\tilde{j} j = a \in \mathfrak{Z}. \tag{40}$$

Moreover $\widetilde{\tilde{j}j} = \tilde{j}j$ and therefore $a \in \mathfrak{Z}_0$, from (38). Now $j^s = b$ and $\tilde{j}^s = \tilde{b}$ and $b\tilde{b} = \tilde{j}^s j^s = aa^{(1)} \cdots a^{(s-1)}$. Thus we arrive at the important condition

$$N_{\mathfrak{R}/\mathscr{L}}(b) = N_{\mathfrak{Z}_0/\mathscr{L}}(a). \tag{41}$$

(See Theorem 18, p.160, [1])

Conversely, if $\mathscr{V}$ is a cyclic algebra generated by 1, $j, j^2, \ldots j^{s-1}$ over its splitting field $\mathfrak{Z}$ and if $\mathfrak{Z}$ is realisable as a field $\mathscr{L}(c, \varsigma)$ as above and further, if $j^s = b$ in $\mathfrak{R}$ satisfies (41) for a suitable $a \in \mathscr{L}(\varsigma)$, then we can define an involution of the second kind in $\mathscr{V}$ as follows. For $\xi = \eta_0 + \eta_1 c$ in $\mathfrak{Z}$ with $\eta_0, \eta_1 \in \mathfrak{Z}_0$, we have only to define

$$\widetilde{\xi} = \eta_0 - \eta_1 c$$

$$\widetilde{j} = a j^{-1} \tag{42}$$

Extending (42) to all elements of $\mathscr{V}$ in the obvious way, we have an involution of the second kind.

We shall now show that Wedderburn's conditions sufficient for a cyclic algebra $\mathscr{V}$ to be a division algebra are not incompatible with condition (41) which is necessary and sufficient for a cyclic (division) alge-
48 bra to carry an involution of the second kind.

Let us take $\mathscr{L} = \mathbb{Q}$, $c = \sqrt{-1}$, $\mathfrak{R} = \mathbb{Q}(\sqrt{-1})$, p an odd prime and ε, a primitive p^{th} root of unity. The field $\mathfrak{Z}_0 = \mathbb{Q}(\varsigma)$ with $\varsigma = \varepsilon + \varepsilon^{-1}$ is cyclic of degree $s = \frac{1}{2}(p-1)$ over $\mathscr{L}$. If now q is a prime $q \equiv 1($ mod 4), then $q = \kappa\overline{\kappa}$ for κ in $\mathfrak{R}$, since $\left(\frac{-1}{q}\right) = 1$. Let us further suppose that q is a primitive root modulo p (There exist infinitely many such q). If now $\mathfrak{Z} = \mathfrak{R}(\varsigma)$, it is clear that the integral ideal (κ) generated by κ in $\mathfrak{Z}$ is prime; similarly $(\overline{\kappa})$ is prime in $\mathfrak{Z}$ and $(\kappa) \neq (\overline{\kappa})$. Now let us define $b = \kappa\overline{\kappa}^{s-1}$. Then $N_{\mathfrak{R}/\mathscr{L}}(b) = N_{\mathfrak{Z}_0/\mathscr{L}}(q)$. Moreover, we claim that for $0 < r < s$, $b^r \neq \xi\xi^{(1)}\cdots\xi^{(s-1)}$ for $\xi \in \mathfrak{Z}_0$. For, otherwise, let $b^r = \xi\xi^{(1)}\cdots\xi^{(s-1)}$ for $\xi \in \xi_0$ and let $\xi = \kappa^t \cdot \lambda$ where in the prime factor decomposition of (λ), (κ) does not occur. Now $\xi^{(1)} = \kappa^t\lambda^{(l)}$ and therefore

$$\kappa^r \cdot \overline{\kappa}^{(s-1)r} = \kappa^{st}\lambda \cdot \lambda^{(1)}\cdots\lambda^{(s-1)}$$

As a consequence $r = st$, which is a contradiction, since $0 < r < s$ and t is a rational integer.

Thus the cyclic algebra generated by $1, j, \ldots, j^{s-1}$ over $\mathfrak{Z}$ as splitting field (where $j^s = b$) is, in fact, a division algebra with an involution of the second kind.

Example. $p = 7$, $s = \dfrac{p-1}{2} = 3$, $q = 17 = (4+i)(4-i)$, $\kappa = 4+i$, $b = (4+i)(4-i)^2$, $a = 17$, $j^3 = b$, $\mathfrak{Z} = \mathbb{Q}\left(\cos\dfrac{2\pi}{7}, i\right)$.

49 Let $\delta \to D$ be the representation of the division algebra over its splitting field, where D is given by (35). Under this representation, we have

$j \to \mathscr{F} = \left(\begin{smallmatrix} 0 & E_{s-1} \\ b & 0 \end{smallmatrix}\right)$, E_{s-1} being the $(s-1)$-rowed identity matrix

and for $\xi \in \mathfrak{Z}$,

$$\xi \to [\xi, \xi^{(1)}, \dots \xi^{(s-1)}]$$

Let now $\delta \to \widetilde{\delta}$ be an involution of the second kind in $\mathscr{V}$ and let $\widetilde{D}$ correspond to $\widetilde{\delta}$ under the representation above. The restriction of the involution in $\mathscr{V}$ to $\mathfrak{Z}$ is an automorphism $\xi \to \overline{\xi}$ of $\mathfrak{Z}$. Let us denote for any matrix $M = (m_{kl})$ with $m_{kl} \in \mathfrak{Z}$, the matrix $(\overline{m}_{kl})$ by $\overline{M}$. Then the connection between D and $\widetilde{D}$ is given by

Proposition 10. *There exists an s-rowed nonsingular symmetric matrix F with elements in $\mathfrak{Z}_0$ such that, for any $\delta \in \mathscr{V}$, we have*

$$\widetilde{D} = F^{-1}\overline{D}'F \tag{43}$$

Proof. Since $\mathscr{V}$ has an involution of the second kind, we have, by (41) an element $a \in \mathfrak{Z}$ such that

$$b\overline{b} = aa^{(1)} \cdot a^{(s-1)} \tag{44}$$

Now to $\widetilde{j} = aj^{-1}$ corresponds $\widetilde{\mathscr{F}} = [a, a^{(1)}, \dots a^{(s-1)}]\begin{pmatrix} 0 & b^{-1} \\ E_{s-1} & 0 \end{pmatrix}$ We shall find elements $x_0, x_1, \dots, x_{s-1}$ in $\mathfrak{Z}_0$ different from zero, such that

$$[x_0, x_1, \dots, x_{s-1}]\begin{pmatrix} 0 & \overline{b} \\ E_{s-1} & 0 \end{pmatrix}[x_0, x_1, \dots, x_{s-1}]^{-1} = \widetilde{\mathscr{F}} = \begin{pmatrix} 0 & \frac{a}{b} \\ [a^{(1)}, \dots, a^{(s-1)}] & 0 \end{pmatrix}$$

This matrix equation is equivalent to the conditions **50**

$$\frac{x_1}{x_0} = a^{(1)}, \dots, \frac{x_{s-1}}{x_{s-2}} = a^{(s-1)}, \quad \frac{x_0\overline{b}}{x_{s-1}} = \frac{a}{b} \tag{45}$$

If we set for $1 \leq i \leq s-1$, $x_i = aa^{(1)} \cdots a^{(i)}$ and $x_0 = a$, then they satisfy (45) and the last condition in (45) is nothing but (44). Thus if we set $F = [a^{-1}, (aa^{(1)})^{-1}, \dots, (aa^{(1)} \cdots a^{(s-1)})^{-1}]$ then $\widetilde{\mathfrak{F}} = F^{-1}\overline{\mathfrak{F}}'F$ and by iteration, we have

$$\widetilde{\mathfrak{F}}^r = F^{-1}\overline{\mathfrak{F}}'^rF \tag{46}$$

For $\xi \in \mathfrak{Z}$, $\xi \to [\xi, \xi^{(1)}, \dots, \xi^{(s-1)}]$ and it is trivial to verify that

$$[\widetilde{\xi}, \widetilde{\xi^{(1)}}, \dots, \widetilde{\xi^{(s-1)}}] = [\overline{\xi}, \overline{\xi^{(1)}}, \dots, \overline{\xi^{(s-1)}}] = F^{-1}[\overline{\xi}, \overline{\xi^{(1)}}, \dots, \overline{\xi^{(s-1)}}]'F \tag{47}$$

From (46) and (47), follows (43) for any $\delta \in \mathscr{V}$. Let us note that F itself does not correspond in general to an element of $\mathscr{V}$ under the representation $\delta \to D$.

The relationship (43) between $\widetilde{D}$ and D will be useful in examining the positivity of the involution $\delta \to \widetilde{\delta}$. Our next object will be to find all involutions of the second kind in $\mathscr{V}$ and to investigate the existence of a positive involution. Results in this direction are again due to Albert [1].

If $\delta \to \delta^*$ is any other involution in $\mathscr{V}$ having the same effect on $\mathfrak{R}$ as the involution $\delta \to \widetilde{\delta}$, then we know that, for a $\lambda \neq 0$ in $\mathscr{V}$ with
51 $\widetilde{\lambda} = \pm\lambda$, $\delta^* = \lambda^{-1}\widetilde{\delta}\lambda$. Since the involutions are of the second kind, we can suppose without loss of generality that $\widetilde{\lambda} = +\lambda$, by taking, if necessary $c\lambda$ instead of λ. Now if $\lambda \to L$ under the representation $\delta \to D$, then this means that $D^* = L^{-1}\widetilde{D}L = L^{-1}F^{-1}\overline{D}'FL$. Setting $G = FL$, we have from $\widetilde{L} = L$ that $G = \overline{G}'$. Thus we have

$$D^* = G^{-1}\overline{D}'G, \quad G = FL = \overline{G}'. \tag{48}$$

□

6 Positive involutions of the second kind in division algebras

Let $\delta \to \widetilde{\delta}$ be an involution of the second kind in a division algebra $\mathscr{V}$ over $\mathbb{Q}$, with centre $\mathfrak{R} \supset \mathbb{Q}$. Then we know from §5 that $\mathscr{V}$ has a splitting field $\mathfrak{Z}$ which can be realised as an abelian extension $\mathscr{L}(c, \varsigma)$ where $\mathscr{L}$ is the fixed field of the involution in $\mathfrak{R}$, $\mathfrak{Z}_0 = \mathscr{L}(\varsigma)$ is cyclic of degree s over $\mathscr{L}$ and $c = \sqrt{-d} = -\widetilde{c} \in \mathfrak{R}$ for an element $d \in \mathscr{L}$.

For the involution $\delta \to \widetilde{\delta}$ to be positive, we should have necessarily that $\mathscr{L}$ is totally real and $-d > 0$; thus $\mathfrak{R}$ should be a totally complex quadratic extension of the totally real field $\mathscr{L}$. For $\xi \in \mathfrak{Z}$, $\widetilde{\xi}$ is just the complex conjugate of ξ. Further ξ_0 is totally real and the involution is identity on $\mathfrak{Z}_0$.

From the representation $\delta \to D$ of $\mathscr{V}$ given by (35) we first get a representation $\delta \to D_0$ of $\mathscr{V}$ over $\mathfrak{R}$ by taking $D_0 = (\Omega \times E_s)[D, D^{(1)}, \ldots, D^{(s-1)}](\Omega \times E_s)^{-1}$ where if $D = (d_{pq})$, $D^{(k)} = \left(d_{pq}^{(k)}\right)$ $(1 \leq k \leq s-1)$, E_s

is the s-rowed identity and $\Omega = \left(\gamma_k^{(l)}\right)(1 \leq k, 1 \leq s)$, $\gamma_1, \ldots, \gamma_s$ being a basis of $\mathfrak{Z}_0$ over $\mathscr{L}$ and serving also as a basis of $\mathfrak{Z}$ over $\mathfrak{R}$. Now let **52** $\omega_1, \ldots \omega_h$ be a basis of $\mathfrak{R}$ over $\mathbb{Q}$ and let $\Omega^* = \left(\omega_p^{(q)}\right)(1 \leq p, q \leq h)$. If $D_0 = (\delta_{kl})$, denote by D_{0i} the corresponding matrix $\left(\delta_{kl}^{(i)}\right)$ for $1 \leq i \leq h$. Then setting $\underline{D} = (\Omega^* \times E_{s^2})[D_{01}, \ldots, D_{oh}](\Omega^* \times E_{s^2})^{-1}$ where E_{s^2} is the s^2-rowed identity matrix, we see that the mapping $\delta \to \underline{D}$ is a representation of $\mathscr{V}$ over $\mathbb{Q}$ by hs^2-rowed matrices. Throughout this section, we shall denote by $(\mathscr{V})$, the image of $\mathscr{V}$ under the representation $\delta \to D$ over $\mathfrak{Z}$.

Let us define, analogously, F_0 by $F_0^{-1} = (\Omega \times E_s) \times [F, F^{(1)}, \ldots, F^{(s-1)}](\Omega \times E_s)'$ and denote by $F_{0i}(1 \leq i \leq h)$ the matrix $\left(f_{kl}^{(i)}\right)$ corresponding to $F_0 = (f_{kl})$. Introducing $\underline{F}$ by the definition $\underline{F}^{-1} = (\Omega^* \times E_{s^2})[F_{01}^{-1}, \ldots, F_{oh}^{-1}](\overline{\Omega^* \times E_{s^2}})'$, we see that $\underline{F}$ is a hs^2-rowed rational symmetric matrix and the relation (43) in terms of $\underline{D}$ and $\underline{F}$ goes over into

$$\widetilde{\underline{D}} = \underline{F}^{-1}\underline{D}'\underline{F}, \quad \underline{F} = \underline{F}' \tag{49}$$

Defining $\underline{G} = \underline{F}\ \ \underline{L}$, we see that (48) goes over into

$$\underline{D}^* = \underline{G}^{-1}\underline{D}'\underline{G} \text{ with } \underline{G} = \underline{F}\ \ \underline{L} = \underline{G}' \tag{50}$$

For the involution $\delta \to \delta^*$ to be positive we must require that for $\delta \neq 0$, $\sigma(\underline{D}\ \ \underline{D}^*) = \sigma(\underline{D}\ \underline{G}^{-1}\underline{D}'\underline{G}) > 0$. Now $\sigma(\underline{D}\ \underline{D}^*) = \sum_{i=1}^{h} \sigma(D_{0i}D_{0i}^*) = tr_{\mathfrak{R}/\mathbb{Q}}(\sigma(D_0D_0^*))$ (By defining $(D_{0i})^* = D_{oi}^*$). Further $\sigma(D_0D_0^*) = s\sigma(DD^*)$ by using the fact that $D^{(1)} = \mathscr{F}D\mathscr{F}^{-1}$ $\left(where \mathscr{F} = \left(\begin{smallmatrix} 0 & E_{s-1} \\ b & 0 \end{smallmatrix}\right)\right)$ and hence, by iteration,

$$D^{(k)} = \mathscr{F}^k D \mathscr{F}^{-k} \tag{51}$$

Now $\overline{\sigma(DD^*)} = \sigma(\overline{D}\ \overline{G}^{-1}D'\overline{G}) = \sigma(G\overline{D}'G^{-1}D) = \sigma(DD^*)$ and there- **53** fore for $D \in \mathscr{V}$, $\sigma(D\ D^*)$ is real. The elements x_{kl} of D are linearly independent over $\mathfrak{R}$ and looking upon them as independent complex variables, we see that $\sigma(DD^*)$ is a hermitian form $f(\ \ , \ldots, x_{kl}., \overline{x}_{kl}, .)$ in the s^2 complex variables x_{kl}. On the other hand, by using the arguments of Proposition 7 the necessary and sufficient condition for $tr_{\mathfrak{R}/\mathbb{Q}}(\sigma(D_0D_0^*))$

to be positive is that $\sigma(D_0 D_0^*) = s\sigma(DG^{-1}\overline{G}'G)$ should be a totally positive-definite hermitian form. Analogously to Lemma 2, the necessary and sufficient condition for this may be seen to be that the hermitian matrix G must be totally positive-Definite over $\mathfrak{Z}$. We have thus proved

Proposition 11. *In terms of the representation $\delta \to D$ of $\mathscr{V}$ over $\mathfrak{Z}$, any positive involution of the second kind in $(\mathscr{V})$ is of the form $D \to G^{-1}\overline{D}'G$ where $G = FL$ is totally positive-definite hermitian and $L = F^{-1}\overline{L}'F$ corresponds to a $\lambda \neq 0$ in $\mathscr{V}$.*

In particular, for the involution $D \to \widetilde{D} = F^{-1}\overline{D}'F$ to be positive, the necessary and sufficient condition is that $F = [a, aa^{(1)}, \ldots aa^{(1)} \cdots a^{(s-1)}]$ is totally positive-definite i.e. $a > 0$.

Suppose a is not totally positive i.e. the involution $\delta \to \widetilde{\delta}$ is not positive. Then we claim that the involution $\delta \to \delta^*$ in $\mathscr{V}$ defined by $j^* = \lambda^{-1}\widetilde{j}\lambda$ and $\xi^* = \widetilde{\xi}$ for $\xi \in \mathfrak{Z}$ is positive for suitably chosen λ in $\mathfrak{Z}_0$.

54 In fact, if we set $\theta = \dfrac{\lambda^{(s-1)}}{\lambda}$, then for $\delta \in \mathscr{V}$, we have $D^* = G^{-1}\overline{D}'G$ where

$$G^{-1} = [a\theta, aa^{(1)}\theta\theta^{(1)}, \ldots, aa^{(1)} \ldots a^{(s-1)}\theta\theta^{(1)} \ldots \theta^{(s-1)}].$$

Now $G = \overline{G}'$, $N_{\mathfrak{Z}_0/\mathscr{L}}(\theta) = 1$ and we have only to choose λ in $\mathfrak{Z}_0$ such that G is totally positive. But we see that

$$G^{-1} = \left[a\frac{\lambda^{(s-1)}}{\lambda}, aa^{(1)}\frac{\lambda^{(s-1)}}{\lambda^{(1)}}, \ldots, aa^{(1)} \cdots a^{(s-1)}\frac{\lambda^{(s-1)}}{\lambda^{(s-1)}}\right].$$

Certainly we can find $\lambda \in \mathfrak{Z}_0$ such that the numbers

$$\frac{a}{\lambda}, \frac{aa^{(1)}}{\lambda^{(1)}}, \ldots, \frac{aa^{(1)} \ldots a^{(s-1)}}{\lambda^{(s-1)}} \tag{52}$$

are all positive, since this merely involves choosing $\lambda \in \mathfrak{Z}_0$ such that $\lambda, \lambda^{(1)}, \ldots, \lambda^{(s-1)}$ have prescribed signs. Further this entails that $\lambda^{(s-1)} > 0$, since by (44), $aa^{(1)} \ldots a^{(s-1)} = b\overline{b} > 0$. Multiplying all the numbers in (52) by $\lambda^{(s-1)} > 0$, we see that the numbers $a\theta, a\theta(a\theta)^{(1)}, a\theta(a\theta)^{(1)} \cdots (a\theta)^{(s-1)}$ are positive and hence G is positive-definite. In a similar way, by properly choosing the signs of the other conjugates of λ over $\mathbb{Q}$, we

can actually ensure that $a\theta > 0$ and hence G is totally positive-definite. Thus the existence of positive involutions of the second kind in $\mathscr{V}$ is ensured.

We have seen that any positive involution in $(\mathscr{V})$ (with $\mathscr{L}$ as the fixed field in $\mathfrak{R}$) is given by $D \to G^{-1}\overline{D}'G$ where $G = FL$ is totally positive-definite hermitian and $L = \widetilde{L} = F^{-1}\overline{L}'F \in (\mathscr{V})$. We shall now find that the real dimension of the linear closure $\mathscr{C}$ of the corresponding $\underline{G}$ in the space of (hs^2)-rowed real square matrices is gs^2, where $g = \frac{h}{2}$. For, $\underline{L}$ is equivalent over the field of complex numbers to $[L_{01}, \ldots, L_{0h}]$ and L_{01} is equivalent to $[L, L^{(1)}, \ldots, L^{(s-1)}]$. From (51), we know that $L, L^{(1)}, \ldots, L^{(s-1)}$ are all equivalent to one another. Looking at the form **55**
of a general L in $(\mathscr{V})$, we see that its elements are linearly independent over $\mathfrak{R}$ and are of the form $\eta + \varsigma\sqrt{d}$ where η, ς are in $\mathfrak{Z}_0$. Pairing off the h conjugates of $\mathfrak{R}$ over $\mathbb{Q}$ as $\mathfrak{R}^{(1)}, \mathfrak{R}^{(2)}(= \overline{\mathfrak{R}^{(1)}}), \ldots, \mathfrak{R}^{(h-1)}, \mathfrak{R}^{(h)}(= \overline{\mathfrak{R}^{(h-1)}})$, we observe that $L_{02} = \overline{L}_{01}, \ldots, L_{0h} = \overline{L}_{0(h-1)}$. Expressing η, ς in terms of a basis $\gamma_1, \ldots, \gamma_s$ of $\mathfrak{Z}_0$ over $\mathscr{L}$, we can thus conclude that the complex dimension of the linear closure of $\underline{L}$ and hence of $\underline{G} = \underline{F}\,\underline{L}$ is gs^2. The condition $G = \overline{G}'$ means that the real dimension of $\mathscr{C}$ is precisely gs^2; the positivity of G is expressed in terms of a finite number of inequalities. Using the fact that the rational numbers are dense in the reals, we can find $L \in (\mathscr{V})$ such that the corresponding $\underline{G} = \underline{F}\,\underline{L}$ is sufficiently close to an element of $\mathscr{C}$ and to secure $G = \overline{G}'$, we have only to take $\frac{1}{2}(L + \widetilde{L})$ instead of L.

We shall, without risk of confusion, denote till the end of this section, the rational representations $\underline{D}$, $\underline{F}$, $\underline{L}$, $\underline{G}$ etc. by D, F, L, G etc. respectively. Let $D \to D^*$ be a positive involution in $(\mathscr{V})$; then $D^* = G^{-1}D'G$ with rational $G = G' > 0$. Now, any other positive involution in $(\mathscr{V})$ is of the form $D \to L^{-1}D^*L$ where $L = L^*$ is in $(\mathscr{V})$ and further GL is positive symmetric. By using Lemma 2, this is equivalent to saying that the eigenvalues of L are real and positive. Such an element L in $(\mathscr{V})$ may be called a *positive element* in $(\mathscr{V})$. A nice characterisation of positive elements is given by the following.

Proposition 12 (Albert [6])**.** *Given a positive involution $D \to D^*$ of $(\mathscr{V})$, any other positive involution in $(\mathscr{V})$ is of the form $D \to L^{-1}D^*L$* **56**

where $L = \sum_{k=1}^{p} L_k L_k^*$ *with* L_k *in* $(\mathscr{V})$ *not all equal to* 0.

Proof. First, let, for $L \in (\mathscr{V}), D \to L^{-1}D^*L$ be a positive involution. Then, from above, we know that all the eigenvalues of L are real and positive. Let r be a root of the characteristic equation $|(xE - L)| = 0$. Then r is a totally positive algebraic number and let $\mathscr{F}$ be the field generated by r over $\mathbb{Q}$. By a theorem of Siegel [19], $r = r_1^2 + r_2^2 + r_3^2 + r_4^2$, where, for $1 \leq k \leq 4$, $r_k = \sum_{l=0}^{N-1} a_{kl} r^l$, $(a_{kl} \in \mathbb{Q})$ and N is the degree of $\mathscr{F}$ over $\mathbb{Q}$. Denoting, for $1 \leq k \leq 4$, the polynomial $\sum_{l=0}^{N-1} a_{kl} t^l$ by $p_k(t)$ and $p_1^2(t) + \cdots + p_4^2(t) - t$ by $p(t)$, we see that $p(r) = 0$. Since r is an eigenvalue of L, $p(r) = 0$ is an eigenvalue of $p(L)$. But $p(L)$, being an element of the division-algebra $(\mathscr{V})$, must consequently be 0. i.e. $L = L_1^2 + L_2^2 + L_3^2 + L_4^2$ where $L_k = p_k(L)(1 \leq k \leq 4)$ are in $(\mathscr{V})$. Now $L = L^*$ implies that $L_k^* = L_k$ i.e.

$$L = L_1 L_1^* + \cdots + L_4 L_4^*.$$

Clearly at least one L_k is different from 0.

Conversely, let, in fact, $L = \sum_{k=1}^{p} L_k L_k^* \neq 0$ with $L_k \in (\mathscr{V})$. Then we claim that the mapping $D \to L^{-1}D^*L$ is a positive involution of (V). That it is an involution is clear. What remains to be shown is that $\sigma(DL^{-1}D^*L) > 0$ for $D \neq 0$ in $(\mathscr{V})$. But now

$$\begin{aligned}
\sigma(DL^{-1}D^*L) &= \sigma(DL^{-1}LL^{*^{-1}}D^*L)(\text{since } L = L^*) \\
&= \sigma(D_1 L D_1^* L)(\text{setting } D_1 = DL^{-1}) \\
&= \sum_{k,l-1}^{p} \sigma(D_1 L_k L_k^* D_1^* L_l L_l^*) \\
&= \sum_{k,l} \sigma(L_l^* D_1 L_k (L_l^* D_1 L_k)^*).
\end{aligned}$$

57 Since $L \neq 0$, at least one $L_k \neq 0$ and hence at least one $L_k^* D_1 L_k \neq 0$ in $(\mathscr{V})$ and by the positivity of the involution $D \to D^*$, we see that the new involution is also positive. □

7 Existence of R-matrices with given commutator-algebra

Let $\mathscr{V}$ be a division algebra over $\mathbb{Q}$ with an involution and let $(\mathfrak{M})$ be a rational representation of $\mathscr{V}$. Then $(\mathfrak{M})$ is equivalent to a multiple, say q times, of the regular representation $(\mathscr{V})$ of $\mathscr{V}$ over $\mathbb{Q}$. If $M \in (\mathfrak{M})$, then we can suppose $M = [\underset{q \text{ times}}{D, \ldots D}] = \underset{q}{D}$ (abbreviating $[\underset{q \text{ times}}{G, \ldots G}]$ as $\underset{q}{G}$). The involution $\delta \to \widetilde{\delta}$ in $\mathscr{V}$ can be described as $M \to \underset{q}{F}^{-1} M' F_q$ where $\underset{q}{F}$ is rational symmetric and $M \in (\mathfrak{M})$. In terms of $(\mathfrak{M})$, the involution $\delta \to \delta^* - \lambda^{-1}\widetilde{\delta}\lambda$ (for $\lambda \neq 0$ in $\mathscr{V}$) is described as $M \to M^* = \underset{q}{G}^{-1} M' \underset{q}{G}$ where $\underset{q}{G} = \underset{q}{F}\underset{q}{L}$, $\underset{q}{L} = \widetilde{\underset{q}{L}} \in (\mathfrak{M})$ and $\underset{q}{G} = \underset{q}{G}'$. If the involution $\delta \to \delta^*$ is positive, then G is positive.

In connection with the existence of an R-matrix with the property that $RM = MR$ for every $M \in (\mathfrak{M})$, we shall first look for a rational nonsingular skew-symmetric matrix A such that for all $M \in (\mathfrak{M})$, we have

$$M^* = A^{-1} M' A \tag{53}$$

and then ask for all A for which (53) is true. But since $M^* = \underset{q}{G}^{-1} M' \underset{q}{G}$, **58**
(53) gives $A\underset{q}{G}^{-1} M' = M' A \underset{q}{G}^{-1}$ i.e. $(A\underset{q}{G}^{-1})' \in (\mathscr{F})$, the commutator-algebra of $(\mathfrak{M})$. Setting $T_0 = (\underset{q}{G}^{-1})' A$, we see that $\underset{q}{G}' T_0 = A = -A' = -T_0' \underset{q}{G}$ i.e.

$$T_0 = -\underset{q}{G}^{-1} T_0' \underset{q}{G} \tag{54}$$

Now, for $T \in (\mathscr{F})$, we can show that $\underset{q}{G}^{-1} T' \underset{q}{G} \in (\mathscr{F})$ and the mapping $T \to \underset{q}{G}^{-1} T' \underset{q}{G}$ is, in fact, an involution of $(\mathscr{F})$. Actually, for $T \in (\mathscr{F})$,

$$\widetilde{T} = \underset{q}{F}^{-1} T' \underset{q}{F} = \underset{q}{L}\underset{q}{G}^{-1} T' \underset{q}{G}\underset{q}{L}^{-1} = \underset{q}{G}^{-1} T' \underset{q}{G}$$

since elements of $(\mathscr{F})$ commute with $\underset{q}{L}$. Thus all the involution in $(\mathscr{V})$ induce the same involution $T \to \widetilde{T}$ in $(\mathscr{F})$. Now, from (54), we have

$T_0 = -\widetilde{T}_0$. The problem then is to find non-singular T in $(\mathscr{F})$ such that $\widetilde{T} = -T$. Given T in $(\mathscr{F})$, $T_1 = \frac{1}{2}(T - \widetilde{T})$ always satisfies $\widetilde{T}_1 = -T_1$. But if we can ensure that T_1 is also non-singular, then we will be through. Let now $T \in \mathscr{F}$ be of the form $(T_{kl})(1 \leq k, l \leq q)$ with T_{kl} being hs^2-rowed rational square matrices. Then, for every $D \in (\mathscr{V})$, we have $DT_{kl} = T_{kl}D$ i.e. T_{kl} belongs to $(\mathscr{V})^*$, the commutator-algebra of $(\mathscr{V})$. If $\widetilde{T}$ should be equal to $-T$, then we must have, in particular, $\widetilde{T}_{kk} = -T_{kk}$ for $1 \leq k \leq q$. If we can find nonsingular T_{11} in $(\mathscr{V})^*$ with $\widetilde{T}_{11} = -T_{11}$,
59 then $T = [T_{11}, \ldots, T_{11}]$ will meet our requirements. Now if $(\mathscr{V})^*$ is not commutative, there always exists at least one $T_2 \neq 0$ (and hence non-singular) for which $\widetilde{T}_2 \neq T_2$ and then we can take $T_{11} = T_2 - \widetilde{T}_2$ $(\neq 0$, since $(\mathscr{V})^*$ is a division-algebra). (If, for every $T_3 \in (\mathscr{V})^*$ we have $\widetilde{T}_3 = T_3$, then for any two elements $T_4, T_5 \in (\mathscr{V})^*$, we would have $T_4T_5 = \widetilde{T}_4\widetilde{T}_5 = \widetilde{T_5T_4} = T_5T_4$)

Taking a basis $\lambda_1, \ldots, \lambda_n$ of $\mathscr{V}$ over $\mathbb{Q}$, for any $\delta \in \mathscr{V}$, we have two representations,

$$\delta \to D \text{ where } \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \delta = D \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

$$\delta \to B \text{ where } \delta(\lambda_1, \ldots \lambda_n) = (\lambda_1, \ldots, \lambda_n)B$$

and further $B = C^{-1}DC$ for a fixed rational nonsingular matrix C. The matrices B' give a regular representation of $(\mathscr{V})^*$. Now $B' = C'D'C'^{-1} = (C'G)D^*(C'G)^{-1}$. Hence the matrices D^* for $\delta \in D$ give an equivalent representation of $(\mathscr{V})^*$. Denoting this equivalent representation itself by $(\mathscr{V})^*$, we see that $(\mathscr{V})$ and $(\mathscr{V})^*$ coincide as sets and their multiplicative structure coincides on their centre (cf. Proposition 6). If the involution in $\mathscr{V}$ is of the second kind, then there exists already in $\mathfrak{R}$, an element c with $c \neq \widetilde{c}$.

If finally the involution is of the first kind and further $\mathscr{V} = \mathfrak{R}$, then the commutator algebra of $\mathscr{V}$ is itself and if $\delta \to D$ is an irreducible representation of $\mathfrak{R}$ over $\mathbb{Q}$, then, by (19)′, $D = \Omega[\sigma^{(1)}, \ldots \delta^{(h)}]\Omega^{-1}$. Taking $T_{kl} = \Omega[\delta_{kl}^{(1)}, \ldots \delta_{kl}^{(h)}]\Omega^{-1}$ with $\delta_{kl} \in \mathfrak{R}(1 \leq k, l \leq q)$ for which the matrix (δ_{kl}) is non-singular and skew-symmetric, we have then that the matrix
60 $A = (\Omega_q\Omega')^{-1}(T_{kl}) = (\Omega'^{-1}[\delta_{kl}^{(1)}, \ldots, \delta_{kl}^{(h)}]\Omega^{-1})$ is clearly rational, non-

singular and skew-symmetric. A necessary and sufficient condition for such a non-singular skew-symmetric matrix (δ_{kl}) over $\mathfrak{R}$ to exist is that q is even. It is easy to verify that dett. $A = N_{\mathfrak{R}/\mathbb{Q}}(\text{dett}(\delta_{kl}))/(\text{dett. }\Omega)^{-2q} \neq 0$ i.e. A is non-singular. If $q = 2p$, for example, we can choose $(\delta_{kl}) = \begin{pmatrix} 0 & E_p \\ -E_p & 0 \end{pmatrix}$, E_p being the p-rowed identity matrix.

Having found a rational skew-symmetric matrix A satisfying (53), we proceed to look for an R-matrix R having $(\mathfrak{M})$ for its commutator-algebra. The following proposition prompts us to look for R in the linear closure $(\underline{\mathscr{F}})$ with respect to the reals of the algebra $(\mathscr{F})$.

Proposition 13. *Any real matrix T for which $TM = MT$ for all $M \in ()$ belongs to $(\underline{\mathscr{F}})$.*

Proof. Writing $T = \sigma_1 T_1^0 + \cdots + \rho_k T_k^0$ with $T_1^0, \ldots, T_k^0$ rational and $\rho_1, \ldots, \rho_k$ being real numbers linearly independent over $\mathbb{Q}$, we see from $TM = MT$ for $M \in (\mathfrak{M})$, that $\sum_{p-1}^{k} \rho_p (T_p^0 M - M T_p^0) = 0$. By the linear independence of the ρ_p over $\mathbb{Q}$, we obtain that

$$T_p^0 \in (\mathscr{F}) \text{ for } 1 \leq p \leq k \text{ i.e. } T \in (\underline{\mathscr{F}}).$$

Denoting by $(\underline{\mathfrak{M}})$ the linear closure of $(\mathfrak{M})$ with respect to the reals, we deduce from Proposition 13 that $(\mathscr{F})$ is precisely the set of all real matrices commuting with all elements of $(\underline{\mathfrak{M}})$.

Our object is then to find $R \in (\underline{\mathscr{F}})$ such that

1) $R^2 = -E$ (E being the identity matrix)

2) $AR = S$ is positive-definite symmetric, and

3) Any rational M for which $MR = RM$ belongs to $(\mathfrak{M})$. **61**

For the moment, we shall agree to ignore condition 3) and look for R satisfying only conditions 1) and 2).

A necessary condition for R to exist is that the involution $M \to M^* = A^{-1}M'A$ in $(\mathfrak{M})$ is positive. In particular, $(\mathscr{V})$ should admit a positive involution

$$D \to D^* = G^{-1}D'G, \text{ where } G = G' > 0 \tag{55}$$

and hence $\mathscr{V}$ has to be one of the following four types:

i) $\mathscr{V} = \mathfrak{R}$, a totally real algebraic number field of degree h over $\mathbb{Q}$.

ii) $\mathscr{V} = \mathcal{G}$, a totally indefinite quaternion algebra over $\mathfrak{R}$ of 1st kind

iii) $\mathscr{V} = \mathscr{F}$, totally definite quaternion algebra over $\mathfrak{R}$ of 1st kind

iv) $\mathscr{V}$ is a cyclic algebra with a positive involution (55) of the second kind, with centre $\mathfrak{R}$ which is a totally imaginary quadratic extension of the fixed field $\mathscr{L}$ of the involution, $\mathscr{L}$ being totally real and of degree g over $\mathbb{Q}$. Further $\mathscr{V}$ has a splitting field $\mathfrak{Z}$ of degree $s \geq 1$ over $\mathfrak{R}$, with $\mathfrak{Z}$ being realisable as indicated at the beginning of §6.

□

For the construction of R, we shall deal with these four cases separately. We shall first find a simple normal form for elements of $(\underline{\mathfrak{M}})$ and then, for elements of $(\underline{\mathscr{F}})$.

Case (i) $\mathscr{V} = \mathfrak{R}$.

For $\mathfrak{R}$, we have the regular representation $\delta(\in \mathfrak{R}) \to D = \left(\omega_k^{(l)}\right)[\delta^{(1)}, \ldots, \delta^{(h)}]\left(\omega_k^{(l)}\right)^{-1}$ with respect to a basis $\omega_1, \ldots, \ldots, \omega_h$ of $\mathfrak{R}$ over $\mathbb{Q}$. The linear closure $(\underline{\mathscr{V}})$ of $(\mathscr{V})$ with respect to the real number field $\mathbb{R}$ consists
62 of all matrices of the form $\left(\omega_k^{(1)}\right)[\delta_1, \ldots \delta_h]\left(\omega_k^{(l)}\right)^{-1}$ where $\delta_1, \ldots, \delta_h$ are arbitrary real numbers. Taking an $\mathbb{R}$-equivalent representation for $(\underline{\mathscr{V}})$ (i.e. a representation equivalent over the reals), we may suppose that $(\underline{\mathfrak{M}})$ consists of all real matrices of the form $\underset{q}{\underline{R}} = [\overset{1}{R}_1, \ldots, \overset{1}{R}_h]$ where $R_1, \ldots, R_h$ are independent one-rowed real square matrices occurring with multiplicity q. The commutator-algebra $(\underline{\mathscr{F}})$ of $(\underline{\mathfrak{M}})$ consists exactly of real matrices $\underset{1}{\underline{T}} = [\overset{q}{T}_1, \ldots, \overset{q}{T}_h]$ where $T_1, \ldots, T_h$ are arbitrary q-rowed real square matrices occurring with multiplicity 1. In passing to the new representation $\delta \to \underline{D} = [\delta_1, \ldots, \delta_h]$ of $(\underline{\mathscr{V}})$, the positive symmetric matrix G in (55) goes over into the h-rowed indentity matrix E_h. The positive involution in $(\mathfrak{M})$ is just $\underset{q}{\underline{R}} \to (\underline{R})^* = \underset{q}{E_h}(\underline{R})'\underset{q}{E_h} = R'$ and the induced involution in $(\underline{\mathscr{F}})$ is just $\underline{T} \to \underline{T}'$.

Case (ii) $\underline{\mathscr{V} = \mathscr{G}}$

Any element $\delta \in \mathscr{G}$ is of the form $x + yi + zj + tk$ where $x, y, z, t \in \Re$, $i^2 = a > 0$, $j^2 = b$, $-b > 0$, $a, b \in \Re$, $\xi = x + yi$, $\overline{\xi} = x - yi$, $\eta = z + ti$, $\overline{\eta} = z - ti$. For $\mathscr{G}$, we have the representation over $\Re$ given by $\delta = \xi + \eta j \to D$ where $D = \left(\left(\begin{smallmatrix} 1 & 1 \\ i & -i \end{smallmatrix}\right) \times E_2\right) [D_1, \overline{D}_1] \times \left(\left(\begin{smallmatrix} 1 & 1 \\ i & -i \end{smallmatrix}\right) \times E_2\right)^{-1}$, $D_1 = \left(\begin{smallmatrix} \xi & \eta \\ b\overline{\eta} & \overline{\xi} \end{smallmatrix}\right)$, $\overline{D}_1 = \left(\begin{smallmatrix} \overline{\xi} & \overline{\eta} \\ b\eta & \xi \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ b & 0 \end{smallmatrix}\right) D_1 \left(\begin{smallmatrix} 0 & 1 \\ b & 0 \end{smallmatrix}\right)^{-1}$. Further $\mathscr{G}$ has a rational representation $\delta \to K[D^{(1)}, \ldots, D^{(h)}]K^{-1}$, K being a certain fixed matrix. Going over to an $\mathbb{R}$-equivalent representation, we see that ($\underline{\mathscr{M}}$) consists of all real matrices of the form $\underline{D} = [\underset{2q}{\overset{2}{R}}_1, \ldots, \underset{2q}{\overset{2}{R}}_h]$ where $R_1, \ldots, R_h$ are arbitrary 2-rowed real square matrices occurring with multiplicity $2q$. Any real matrix commuting with all real matrices of the form $\underset{2q}{R}$ **63** where R is a real 2-rowed square matrix, is of the form (T_{kl}) $(1 \leq k, l \leq 2q)$ with $T_{kl} = t_{kl}E_2$, $t_{kl} \in \mathbb{R}$. Thus ($\mathscr{F}_1$) consists of all the matrices of the form $\underline{T} = [\underset{2q}{T_1} \times E_2, \ldots, \underset{2q}{T_h} \times E_2]$ where $T_1, \ldots, T_h$ are arbitrary $2q$-rowed real square matrices. The positive involution in $\mathscr{G}$ is given by $D_1 \to D_1^* = G_1^{-1} D_1' G_1$ where G_1 is symmetric and totally-positive over $\Re$. This involution goes over in ($\underline{\mathscr{M}}$) to the involution $\underline{D} \to \underline{D}^* = \left[\underset{2q}{G_1^{(1)^{-1}}} \underset{2q}{\overset{2}{R}}_1' \underset{2q}{G_1^{(1)}}, \ldots, \underset{2q}{G_1^{(h)^{-1}}} \underset{2q}{\overset{2}{R}}_h' \underset{2q}{G_1^{(h)}}\right]$. For each $G_1^{(k)} (l \leq k \leq h)$, there exists a real non-singular matrix C_k such that $G_{1_2}^{(k)} = C_k' C_k$. Taking for ($\mathscr{M}$), the equivalent representation $\underline{D} = \left[\underset{2q}{C_1} \underset{2q}{R_1} \underset{2q}{C_1^{-1}}, \ldots, \underset{2q}{C_h} \underset{2q}{\overset{2}{R}}_h \underset{2q}{C_h^{-1}}\right]$, we see that ($\mathscr{M}$) still consists of the same set of matrices as above but, in terms of the new representation, the given positive involution is more simply expressed by $\underline{D} \to \underline{D}'$ and the induced involution in ($\underline{\mathscr{F}}$) is just $\underline{T} \to \widetilde{\underline{T}} = \underline{T}'$.

Case (iii) $\mathscr{V} = \Re$

For $\delta = x + yi + zj + tk \in \mathscr{V}$, we have the 4-rowed representation

$$\text{over } \mathfrak{R},\ \text{viz. } \delta \to D = \begin{pmatrix} x & y & z & t \\ ay & x & at & z \\ bz & -bt & x & -y \\ -abt & bz & -ay & x \end{pmatrix} \text{ and a rational}$$

representation given by $\delta \to K_1[D^{(1)}, \ldots, D^{(h)}]K_1^{-1}$ with a constant matrix K_1. It is easy to see after passing to an equivalent representation that $(\mathscr{M})$ consists precisely of all matrices of the form $\underline{D} = [\underset{q}{D_1}, \ldots, \underset{q}{D_h}]$,

64 where $D_1, \ldots D_h$ are matrices of the same form as D above, except that now x, y, z, t are arbitrary real numbers. Let

$$C_k = \left[1,\ \sqrt{-a^{(k)}},\ \sqrt{-b^{(k)}},\ \sqrt{a^{(k)}b^{(k)}}\right] \text{ and } C = [C_1, \ldots, C_h].$$

Taking $C^{-1}\underline{D}C$ instead of $\underline{D}$ and replacing x, y, z, t by x, $\dfrac{y}{\sqrt{-a}}$, $\dfrac{z}{\sqrt{-b}}$, $\dfrac{t}{\sqrt{ab}}$ respectively, we obtain finally that $(\mathscr{M})$ consists of all real matrices of the form $\underline{D} = [\underset{q}{H_1}, \ldots, \underset{q}{H_h}]$ where $H_1, \ldots, H_h$ are independent 4-rowed real representations of Hamiltonian quaternions, each occurring with multiplicity q. Let $\mathbb{K}$ denote the algebra of real Hamiltonian and $(\mathbb{K})$ denote the algebra of 4-rowed real matrices

$$H = \begin{pmatrix} x & y & z & t \\ -y & x & -t & z \\ -z & t & x & -y \\ -t & -z & y & x \end{pmatrix}$$

(with real x, y, z, t) representing elements of $\mathbb{K}$. Then the matrices

$$\widehat{H} = \begin{pmatrix} x & y & z & t \\ -y & x & t & -z \\ -z & -t & x & y \\ -t & z & -y & x \end{pmatrix}$$

(with x, y, z, t real) give a representation of $\widehat{K}$, the opposite algebra of $\mathbb{K}$. We denote by $(\mathbb{K})$ the set of such matrices $\widehat{H}$.

The involution in $\mathfrak{R}$ was, to start with, given by $D \to F^{-1}D'F$ where $F^{-1} = [1, -a, -b, ab]$ and in terms of the new representation, F is to be replaced by the identity. Thus the positive involution in $(\mathscr{M})$ is given by $\underline{D} \to \underline{D}'$. The commutator-algebra $(\mathscr{F})$ consists of all matrices $\underline{T}$ of the form $\underline{T} = [\overset{q}{\underset{1}{\widehat{H}_1}}, \ldots \overset{q}{\underset{1}{\widehat{H}_h}}]$ where, for $1 \leq k \leq h$, $\overset{q}{\widehat{H}_k}$ is an arbitrary q-rowed square matrix with elements which belong to $(\mathbb{K})$ and the involution in $(\mathscr{F})$ is just $\underline{T} \to \underline{T}'$.

Case (iv) *$\mathscr{V}$, a cyclic algebra with a positive involution of the second kind.* **65**

For $\delta \in \mathscr{V}$, we have the regular representation $\delta \to D$ over $\mathfrak{Z}$ given by (35) and the rational representation $\delta + \underline{D}$ (see p. 37). We arrange the conjugates of $\mathfrak{R}$ over $\mathbb{Q}$ as $\mathfrak{R} = \mathfrak{R}^{(1)}, \mathfrak{R}^{(2)} = \overline{\mathfrak{R}^{(1)}}, \ldots, \mathfrak{R}^{(h-1)}, \mathfrak{R}^{(h)} = \overline{\mathfrak{R}^{(h-1)}}$. Using (51) and passing to an equivalent representation over the field $\mathbb{C}$ of complex numbers, we see that the linear closure $(\underline{\mathscr{V}})$ of $(\mathscr{V})$ (with respect to the reals) consists of all complex matrices $\underline{M}$ of the form $\underline{M} = [\overset{s}{\underset{s}{D_1}}, \overline{\overset{s}{\underset{s}{D_1}}}, \overset{s}{\underset{s}{D_3}}, \overline{\overset{s}{\underset{s}{D_3}}}, \ldots, \overset{s}{\underset{s}{D_{h-1}}}, \overline{\overset{s}{\underset{s}{D_{h-1}}}}]$ where D_1, $D_3, \ldots, D_{h-1}$ are g independent s-rowed complex square matrices occurring with multiplicity s. The positive involution $D \to D^* = G^{-1}\overline{D}'G$ in $(\mathscr{V})$ corresponds exactly to a positive involution $\underline{M} \to P^{-1}\overline{M}'P$ in $(\mathscr{V})$ where $P = [\overset{s}{G_1}, \overset{s}{G_2}, \ldots \overset{s}{G_{sh}}]$ is positive-definite hermitian. Now, for a complex non-singular L_k, we have $G_k = \overline{L}_k'L_k$ for $1 \leq k \leq hs$. Let $L = [L_1, L_2, \ldots, L_{sh}]$. Taking the representation $L\underline{M}L^{-1}$ instead of $\underline{M}$, the given involution in $(\mathscr{V})$ is expressed simply by $\underline{M} \to \overline{\underline{M}}'$. Now, every complex matrix $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{smallmatrix}\right)$ with $\alpha = \beta + \sqrt{-1}\gamma (\beta, \gamma$ real) is equivalent over $\mathbb{C}$ to $\left(\begin{smallmatrix} \beta & \gamma \\ -\gamma & \beta \end{smallmatrix}\right)$. Thus passing to a suitable equivalent representation we obtain that $(\mathscr{M})$ consists precisely of all matrices of the form $\underline{D} = [\overset{s}{\underset{sq}{C_1}}, \ldots, \overset{s}{\underset{sq}{C_g}}]$ where $C_1, \ldots, C_g$ are independent s-rowed square matrices with elements which are 2-rowed real representations of complex numbers, each C_i occurring with multiplicity sq. The positive involu-

tion in $(\mathscr{M})$ is just $\underline{D} \to \underline{D}'$. The commutator-algebra $(\mathscr{F})$ consists of
66 all matrices $\underline{T} = [\overset{sq}{T_1} \times E_s, \ldots, \overset{sq}{T_g} \times E_s]$ where $T_1, \ldots, T_g$ are independent sq-rowed square matrices with elements which are 2-rowed real representations of complex numbers. The involution $\underline{T} \to \widetilde{\underline{T}}$ in $(\mathscr{F})$ induced by the positive involution in $(\mathscr{M})$ is just $\underline{T} \to \underline{T}'$. We have thus proved

Theorem 5. *With the notation as above, we have the following normal forms for elements of* $(\mathscr{M})$ *and* $(\mathscr{F})$, viz.

Case (i) $\mathscr{V} = \mathfrak{R}$	$D = [\overset{1}{R_1}, \overset{(\mathscr{M})}{\ldots}, \overset{1}{R_h}]$	$\underline{T} = [\overset{q}{T_1}, \overset{(\mathscr{F})}{\ldots}, \overset{q}{T_h}]$
	$q \qquad\qquad q$	$1 \qquad\qquad 1$
Case (ii) $\mathscr{V} = \mathscr{G}$	$\underline{D} = [\overset{2}{R_1}, \ldots, \overset{2}{R_h}]$	$\underline{T} = [\overset{2q}{T_1} \times E_2, \ldots, \overset{2q}{T_h} \times E_2]$
	$2q \qquad\qquad 2q$	
Case (iii) $\mathscr{V} = \mathfrak{R}$	$\underline{D} = [\overset{1}{H_1}, \ldots, \overset{1}{H_h}]$	$\underline{T} = [\overset{q}{\widehat{H}_1}, \ldots, \overset{q}{\widehat{H}_h}]$
	$q \qquad\qquad q$	$1 \qquad\qquad 1$
Case (iv) $\mathscr{V}$, *cyclic algebra*	$\underline{D} = [\overset{s}{C_1}, \ldots, \overset{s}{C_g}]$	$\underline{T} = [\overset{sq}{C_1} \times E_s, \ldots, \overset{sq}{C_g} \times E_s]$
	$sq \qquad\qquad sq$	

In all the four cases, the given positive involution in $(\mathscr{M})$ *is given by* $\underline{D} \to \underline{D}'$ *and the involution in* $(\mathscr{F})$ *is* $\underline{T} \to \underline{T}'$.

At the beginning of this section, we looked for a rational matrix $A = \underset{q}{G}\, T_0$ with $\widetilde{T}_0 = -T_0$ in $(\mathscr{F})$. With the simplification carried out above in $(\underline{\mathscr{F}})$, we shall reduce $A = T_0$ to a simple normal form by making the real linear transformations in $(\underline{\mathscr{F}})$. For reducing A to the simplest form, we deal with each one of the four cases separately. We denote, in the sequel, the matrix $\left(\begin{smallmatrix} 0 & E_k \\ -E_k & 0 \end{smallmatrix}\right)$ by ϵ_k (E_k being the k-rowed identity) and shall denote ϵ_1 by ϵ, for brevity.

Case (i) $\underline{\mathscr{V} = \mathfrak{R}}$**.** We have seen that a necessary and sufficient condition for such an A to exist is that q is even, say, $q = 2p$. Let $A =$
67 $[\overset{q}{T_1}, \ldots, \overset{q}{T_h}]$ where $T_1, \ldots, T_h$ are arbitrary $2p$-rowed real nonsingular skew-symmetric matrices. By passing to an equivalent representation of $(\mathscr{F})$ (which does not disturb the form of the elements of $(\underline{\mathscr{F}})$, we can suppose that $A = \underset{h}{\epsilon_p}$ already.

Case (ii) $\mathscr{V} = \mathscr{G}$. As in case (i), passing to an equivalent representation of $(\underline{\mathscr{F}})$ which does not destroy the form of the elements of $(\mathscr{F})$, we could suppose that $A = \underset{2h}{\epsilon_q}$.

Case (iii) $\mathscr{V} = \mathscr{P}$. For the sake of simplification, we might, to start with, use for the Hamiltonian quaternions, the representation, as elements of the opposite algebra $(\overline{\mathbb{K}})$. Thus, the elements of $(\underline{\mathscr{F}})$ are exactly all matrices of the form $\underline{T} = [\underset{1}{\overset{q}{H}}_1, \ldots, \underset{1}{\overset{q}{H}}_h]$ where $H_1, \ldots, H_h$ are q-rowed square matrices with elements in $(\mathbb{K})$. We now make a simple transformation in $(\underline{\mathscr{F}})$ as follows (Of course, we have to make a corresponding transformation also in $(\underline{\mathscr{M}})$, in order that $(\underline{\mathscr{F}})$ might continue to be the commutator-algebra of $(\underline{\mathscr{M}})$, but, for the moment, we can afford to forget $(\underline{\mathscr{M}})$). If $H \in (\mathbb{K})$ corresponds to the Hamiltonian quaternion $x + yi + zj + tk = \xi + \eta j$ (where $\xi = x + yi$, $\eta = z + ti$ are in $\mathbb{C}$ and $x, y, z, t \in \mathbb{R}$), then H is nothing but $\left(\begin{smallmatrix} \xi & \eta \\ -\overline{\eta} & \overline{\xi} \end{smallmatrix}\right)$ where ξ, η, $\overline{\xi}$, $-\overline{\eta}$ are just the two-rowed real representations of the corresponding complex numbers. Passing to an equivalent representation for $(\underline{\mathscr{F}})$ with a suitable permutation matrix, we can suppose that the elements of $(\underline{\mathscr{F}})$ are of the form

$$\underline{T} = \left[\begin{pmatrix} C_{1,1} & C_{1,2} \\ -\overline{C}_{1,2} & \overline{C}_{1,1} \end{pmatrix}, \ldots, \begin{pmatrix} C_{h,1} & C_{h,2} \\ -\overline{C}_{h,2} & \overline{C}_{h,1} \end{pmatrix}\right]$$

where $C_{k,l} (1 \leq k \leq h, l = 1, 2)$ are independent q-rowed square matrices **68**
with elements which are of the form $\left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right)$ with $x, y \in \mathbb{R}$. Further $\overline{C_{k,l}}$ is obtained from $C_{k,l}$ by just replacing a general element $\left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right)$ in $C_{k,l}$ by $\left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right)$. Let us consider each one of the h blocks $\left(\begin{smallmatrix} C_{k,1} & C_{k,2} \\ -\overline{C}_{k,2} & \overline{C}_{k,1} \end{smallmatrix}\right)$ in $\underline{T}$, separately. By applying a suitable permutation-transformation to $C_{k,l}$ which brings all the elements x together, all the y together, all the elements $-x$ together and all the elements $-y$ together, we could suppose that $C_{k,l} = \left(\begin{smallmatrix} U_{k,l} & V_{k,l} \\ -V_{k,l} & U_{k,l} \end{smallmatrix}\right)$ where $U_{k,l}$ and $V_{k,l}$ are independent q-rowed real square matrices then $\overline{C}_{k,l} = \left(\begin{smallmatrix} U_{k,l} & -V_{k,l} \\ V_{k,l} & U_{k,l} \end{smallmatrix}\right)$. To start with A is an element of $(\underline{\mathscr{F}})$ satisfying $A = -A'$. By means of a transformation which does not disturb the final form of the elements of $(\underline{\mathscr{F}})$, we can suppose $A = \underset{h}{\epsilon_{2q}}$ already.

Case (iv) *$\mathscr{V}$, a cyclic algebra with a positive involution of the second kind.*

Let $T_0 = [\underset{s}{\overset{sq}{T_1}}, \ldots, \underset{s}{\overset{sq}{T_g}}]$ be a non-singular skew-symmetric matrix in ($\underline{\mathscr{F}}$). Now $\underset{sq}{\epsilon}$ commutes with T_k and $M_k = \underset{sq}{\epsilon} T_k (1 \leq k \leq g)$ considered as a sq-rowed complex matrix is hermitian and non-singular. There exists a sq-rowed complex non-singular matrix L_k such that $\overline{L}_k' M_k L_k = [\underset{a_k}{1}, \underset{b_k}{-1}]$ with $a_k + b_k = sq$. Let $L = [\underset{s}{\overset{sq}{L_1}}, \ldots, \underset{s}{\overset{sq}{L_g}}]$ where, now in L_i, we have replaced the complex elements by their 2-rowed real representations. Taking the equivalent representation $L(\underline{\mathscr{F}})L^{-1}$ instead of ($\underline{\mathscr{F}}$), we see that the elements of ($\underline{\mathscr{F}}$) are again of the same form as above but the matrix T_0 assumes the very simple form $\left[[\underset{a_1}{\epsilon}, \underset{b_1}{-\epsilon}], \ldots, [\underset{a_h}{\epsilon}, \underset{b_h}{-\epsilon}]\right]$. We make now a simple transformation on ($\underline{\mathscr{F}}$). The elements of ($\underline{\mathscr{F}}$) are of the form $[\underset{s}{\overset{sq}{T_1}}, \ldots, \underset{s}{\overset{sq}{T_g}}]$ where each T_i is a sq-rowed matrix with elements of the form $\left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right)$, $x, y \in \mathbb{R}$. Passing to an equivalent representation of ($\mathscr{F}$), by clubbing all the x's together and all the y's together as in case (iii), we may suppose that each $T_k = \left(\begin{smallmatrix} U_k & V_k \\ -V_k & U_k \end{smallmatrix}\right)$ where U_k, V_k are arbitrary sq-rowed real square matrices. Thus T_0 goes over into $[\underset{s}{\overset{0}{T_1^0}}, \ldots, \underset{s}{\overset{0}{T_g^0}}]$ where $T_k^0 = \left(\begin{smallmatrix} 0 & P_k \\ -P_k & 0 \end{smallmatrix}\right)$ $(1 \leq k \leq g)$ and $P_k = [\underset{a_k}{1}, \underset{b_k}{-1}]$ with $a_k + b_k = sq$. As a further simplification, we take the representation $B(\underline{\mathscr{F}})B^{-1}$ where $B = [\underset{s}{B_1}, \ldots, \underset{s}{B_g}]$ and $B_k = [\underset{sq}{1}, P_k] (1 \leq k \leq g)$. Thus ($\underline{\mathscr{F}}$) may be supposed to be the set of all matrices of the form $[\underset{s}{\overset{sq}{\widehat{C}_1}}, \ldots, \underset{s}{\overset{sq}{\widehat{C}_g}}]$ where $\widehat{C}_k = \left(\begin{smallmatrix} U_k & V_k & P_k \\ -P_k V_k & P_k U_k & P_k \end{smallmatrix}\right) (1 \leq k \leq g)$ and U_k, V_k are arbitrary sq-rowed real square matrices. Our given matrix T_0 goes over into the simple matrix $[\underset{s}{\epsilon_{sq}}, \ldots, \underset{s}{\epsilon_{sq}}]$.

Summing up, the elements of ($\underline{\mathscr{F}}$) have the normal form given in the following table and in each of the four cases, the given matrix T_0 in

($\underline{\mathscr{F}}$) assumes the simple form J.

	($\underline{\mathscr{F}}$)	J_0	$\underline{\mathrm{J}}$
$\mathscr{V} = \mathfrak{R}$	$\underline{T} = [\overset{2p}{\underset{1}{R_1}}, \ldots, \overset{2p}{\underset{1}{R_h}}]$	ϵ_p	$\underset{h}{\mathrm{J}_0}$
$\mathscr{V} = \mathscr{G}$	$\underline{T} = [\overset{2q}{\underset{2}{R_1}}, \ldots, \overset{2q}{\underset{2}{R_h}}]$	ϵ_q	$\underset{2h}{\mathrm{J}_0}$
$\mathscr{V} = \mathfrak{R}$	$\underline{T} = [\overset{q}{\underset{1}{H_1}}, \ldots, \overset{q}{\underset{1}{H_h}}]$ where H_k is of the form $\begin{pmatrix} C_1 & C_2 \\ -\overline{C}_2 & \overline{C}_1 \end{pmatrix}, C_1 = \begin{pmatrix} U & V \\ -V & U \end{pmatrix}$ and $\overline{C}_1 = \begin{pmatrix} U & -V \\ V & U \end{pmatrix}$	ϵ_{2q}	$\underset{h}{\mathrm{J}_0}$
$\mathscr{V}$, *cyclic algebra*	$\underline{T} = [\overset{sq}{\underset{s}{\widehat{C}_1}}, \ldots, \overset{sq}{\underset{s}{\widehat{C}_g}}]$ where $\widehat{C}_k$ is of the form $\begin{pmatrix} U_k & V_k P_k \\ -P_k V_k & P_k U_k P_k \end{pmatrix}$, and $P_k = [\underset{a_k}{1}, \underset{b_k}{-1}]$ with $a_k + b_k = sq$	ϵ_{sq}	$\underset{sq}{\mathrm{J}_0}$

(56)

70

We have to find $R \in (\underline{\mathscr{F}})$ such that $R^2 = -E$ and $\mathrm{J}R = S = S' > 0$. Since R and J are both in ($\underline{\mathscr{F}}$), they decompose into similar blocks and therefore confining ourselves to one of the components at a time, our problem reduces to finding all real matrices R satisfying

$$\mathrm{J}_0 R = S = S' > 0, \quad R^2 = -E \tag{57}$$

and further R is of the form $\overset{2p}{R_1}$, $\overset{2q}{R_1}$, $\overset{q}{H_1}$ or $\overset{sq}{\widehat{C}_1}$ as in (56). We shall call a real matrix R of the form $\overset{2p}{R_1}$, $\overset{2q}{R_1}$, $\overset{q}{H_1}$ or $\overset{sq}{\widehat{C}_1}$ as in (56), an *admissible matrix of type* 1, 2, 3 or 4 respectively.

From (56), we get $\mathrm{J}_0^{-1} S \mathrm{J}_0^{-1} S = -E$, $S = S' > 0$. Since $\mathrm{J}_0^2 = -E$, we have

$$S \mathrm{J}_0 S = \mathrm{J}_0, \quad S = S' > 0. \tag{58}$$

Thus we have to look for all *admissible positive symmetric symplectic* matrices S.

Let us now analyse (58). First note that $E + S$ is positive symmetric along with S. Let us set $W = 2(E + S)^{-1}$; then W is positive symmetric too and further $S = -E + 2W^{-1}$. From (58), we get **71**

$$4W^{-1}\mathrm{J}_0 W^{-1} - 2W^{-1}\mathrm{J}_0 - 2\mathrm{J}_0 W^{-1} = 0, \quad \text{i.e. } 2\mathrm{J}_0 = \mathrm{J}_0 W + W\mathrm{J}_0.$$

Setting $\mathsf{J}_0 - \mathsf{J}_0 W = -F$, this means that $F = F'$. Further F is admissible, of the same type as J_0 and W. Let us write

$$F = \begin{pmatrix} G & H \\ H' & K \end{pmatrix} \text{ with } G = G', K = K'$$

G and K having the same number of rows. Now $W = E - \mathsf{J}_0 F$, $W = W'$ together give $\mathsf{J}_0 F = (\mathsf{J}_0 F)'$. But $\mathsf{J}_0 F = \left(\begin{smallmatrix} H' & K \\ -G & -H \end{smallmatrix}\right)$. Thus $H = H'$ and $K = -G$. Now $S = -E + 2(E - \mathsf{J}_0 F)^{-1} = (E + \mathsf{J}_0 F)(E - \mathsf{J}_0 F)^{-1}$. Thus

$$R = \mathsf{J}_0^{-1} S = +\mathsf{J}_0^{-1}(E + P)(E - P)^{-1} \tag{59}$$

where

$$P = \begin{pmatrix} H & -G \\ -G & -H \end{pmatrix}, \quad H = H', \quad G = G'. \tag{60}$$

and P is admissible, of one of the four types. (The parametrization of S is quite similar to the Cayley parametric representation for orthogonal matrices).

We now proceed to examine the nature of the set of all admissible R satisfying $R^2 = -E$ and $\mathsf{J}_0 R = (\mathsf{J}_0 R)' > 0$, distinguishing between the various types. For this purpose, we go back to the Riemann matrices associated with the R-matrix R. From § 1, we know that we can find a Riemann matrix $\mathscr{P}$ uniquely up to a left-sided complex non-singular matrix factor such that

$$R = \begin{pmatrix} \mathscr{P} \\ \overline{\mathscr{P}} \end{pmatrix}^{-1} \begin{pmatrix} -iE & 0 \\ 0 & iE \end{pmatrix} \begin{pmatrix} \mathscr{P} \\ \overline{\mathscr{P}} \end{pmatrix}, \quad \mathscr{P} \mathsf{J}_0^{-1} \mathscr{P}' = 0, \quad i \mathscr{P} \mathsf{J}_0^{-1} \overline{\mathscr{P}}' > 0. \tag{61}$$

72 (Here $i = \sqrt{-1}$). If $\mathscr{P} = (AB)$ with square matrices A and B, then we know that A, B are both non-singular and hence, we can assume without loss of generality, that $\mathscr{P} = (Z\ E)$ and the last two conditions in (61) are, in terms of Z, just

$$Z = X + iY, \quad X = X', \quad Y = Y', \quad Y > 0. \tag{62}$$

From (59), (60) and the first condition in (61) we obtain

$$\begin{pmatrix} \mathscr{P} \\ \overline{\mathscr{P}} \end{pmatrix} \mathsf{J}_0^{-1}(E + P) = \begin{pmatrix} -iE & 0 \\ 0 & iE \end{pmatrix} \begin{pmatrix} \mathscr{P} \\ \overline{\mathscr{P}} \end{pmatrix} (E - P)$$

i.e.

$$\begin{aligned} -iZ + iZH - iG &= ZG + E + H \\ -iZG - iE - iH &= -Z + ZH - G \\ \overline{Z}(-iE + iH - G) &= E + H + iG \\ \overline{Z}(iG + E - H) &= -G - iE - iH \end{aligned} \tag{63}$$

Let us set $Z_0 = H + iG$. Then solving for Z_0 from the third equation in (63), we have $E + Z_0 = Z(-iE + iZ_0)$, i.e. $(E - iZ)Z_0 = -(E + iZ)$. (equivalently, $Z = i(E + Z_0)(E - Z_0)^{-1}$)

$$\begin{aligned} Z_0 = Z_0' &= -(E - iZ)^{-1}(E + iZ) \\ &= -(E + iZ)(E - iZ)^{-1} \end{aligned} \tag{64}$$

The condition $S > 0$ is equivalent to $Y > 0$ and using (63), this is equivalent to

$$E - \overline{Z}_0 Z_0 > 0. \tag{65}$$

The mapping $Z \to Z_0$ takes the "*generalized upper half-plane of degree n*" consisting of all n-rowed complex Z satisfying (62) into the "generalized unit circle" consisting of all n-rowed $Z_0 = Z_0'$ satisfying (65). **73**

Thus R is an admissible matrix of the form

$$R = \mathrm{J}_0^{-1} \begin{pmatrix} E + H & -G \\ -G & E - H \end{pmatrix} \begin{pmatrix} E - H & G \\ G & E + H \end{pmatrix}^{-1} \tag{66}$$

where $Z_0 = H + iG$ satisfies

$$Z_0 = Z_0', \quad E - \overline{Z}_0 Z_0 > 0 \tag{67}$$

In case $\mathscr{V} = \mathfrak{R}$ or $\mathscr{V} = \mathscr{G}$, any q-rowed (respectively $2q$-rowed) real square matrix is admissible and therefore, from (60), G, H can be arbitrary real square matrices of $\frac{q}{2}$ and q rows respectively. Thus $Z_0 = H + iG$ is an arbitrary point of the generalized unit circle of degree $\frac{q}{2}$ in case $\mathscr{V} = \mathfrak{R}$ and of degree q, in case $\mathscr{V} = \mathscr{G}$. The matrix Z is then an arbitrary point of the generalized upper half-plane of the corresponding

degree. Taking into account all the components in the representation (56) of ($\mathscr{F}$), we are led in the case $\mathscr{V} = \Re$, to a h-fold product of the generalized upper half-plane of degree $\frac{q}{2}$ which is a complex space of complex dimension $\frac{h}{2}\left(\frac{q}{2}+1\right)\frac{q}{2}$. In the case $\mathscr{V} = \mathscr{G}$ we arrive at the h-fold product of the generalized upper half-plane of degree q, which is of complex dimension $\frac{h}{2}q(q+1)$.

Let us take the case $\mathscr{V} = \Re$. From the form (60) of P and from the 'admissibility' of P, we see that $H = H' = -\overline{H}$, $G = G' = -\overline{G}$ and both G and H have to be of the form $\left(\begin{smallmatrix} U & V \\ -V & U \end{smallmatrix}\right)$ with U, V being arbitrary q-rowed real square matrices. From $H' = -\overline{H}$, $G' = -\overline{G}$, we obtain $H =$
74 $\left(\begin{smallmatrix} 0 & X_1 \\ X_1' & 0 \end{smallmatrix}\right)$, $G = \left(\begin{smallmatrix} 0 & Y_1 \\ Y_1' & 0 \end{smallmatrix}\right)$ with $X_1 = -X_1'$ and $Y_1 = -Y_1'$. Now $Z_0 = \left(\begin{smallmatrix} 0 & Z_1 \\ Z_1' & 0 \end{smallmatrix}\right)$ with $Z_1 = X_1 + iY_1 = -Z_1'$. Condition (65) is equivalent to the condition $E - \overline{Z}_1 Z_1' > 0$. We are thus led, in this case, to the set of q-rowed complex square matrices Z_1 satisfying

$$Z_1' = -Z_1, \quad E_q - \overline{Z}_1 Z_1' > 0 \tag{68}$$

This space, like the 'generalized unit circle' met before in earlier cases, is again one of the complex symmetric spaces of E. Cartan. It is of complex dimension $q(q-1)/2$. If we take into account all the components in the representation (56) of ($\mathscr{F}$), we are led to a h-fold product of the symmetric domain defined by (68). We remark that there is no special advantage in interpreting (68) in terms of Z and in fact, it becomes more complicated.

We now take up case (iv). Since P is admissible of type 4, it follows that

$$H = -DHD,\ G = -DGD \text{ where } D = [\underset{a}{1}, \underset{b}{-1}] \text{ with } a + b = sq.$$

Breaking up H as $\left(\begin{smallmatrix} H_1 & H_2 \\ H_3 & H_4 \end{smallmatrix}\right)$ with a-rowed square H_1, we see that $H = H' = -DHD$ implies $H_4 = 0$, $H_1 = 0$, $H_2 = H_3'$. Thus $H = \left(\begin{smallmatrix} 0 & X_2 \\ X_2' & 0 \end{smallmatrix}\right)$ and similarly $G = \left(\begin{smallmatrix} 0 & Y_2 \\ Y_2' & 0 \end{smallmatrix}\right)$ with arbitrary real X_2, Y_2 of $\underline{a}$ rows and $\underline{b}$ columns. Now $Z_0 = H + iG = \left(\begin{smallmatrix} 0 & Z_2 \\ Z_2' & 0 \end{smallmatrix}\right)$ with $Z_2 = X_2 + iY_2$ having $\underline{a}$ rows and $\underline{b}$

columns. Condition (65) is equivalent to the two conditions,

$$E_a - \overline{Z}_2 Z_2' > 0, \quad E_b - \overline{Z}_2' Z_2 > 0 \tag{69}$$

Now "$E_a - \overline{Z}_2 Z_2' > 0$" is equivalent to the fact that the matrix **75**

$$M = \begin{pmatrix} E_a & \overline{Z}_2 \\ Z_2' & E_b \end{pmatrix} = \begin{pmatrix} E_a & \overline{Z}_2 \\ 0 & E_b \end{pmatrix} \begin{pmatrix} E_a - \overline{Z}_2 Z_2' & 0 \\ 0 & E_b \end{pmatrix} \begin{pmatrix} E_a & 0 \\ Z_2' & E_b \end{pmatrix}$$

is positive-hermitian. But $M > 0$ if and only if $\overline{M} > 0$. On the other hand

$$\overline{M} = \begin{pmatrix} E_a & 0 \\ \overline{Z}_2' & E_b \end{pmatrix} \begin{pmatrix} E_a & 0 \\ 0 & E_b - \overline{Z}_2' Z_2 \end{pmatrix} \begin{pmatrix} E_a & Z_2 \\ 0 & E_b \end{pmatrix}$$

is positive-hermitian if and only if $E_b - \overline{Z}_2' Z_2 > 0$. Thus the two conditions in (69) reduce to the single condition

$$E_a - \overline{Z}_2 Z_2' > 0 \tag{69}'$$

The set of complex rectangular matrices Z_2 of $\underline{a}$ rows and $\underline{b}$ columns satisfying (69)′ is again a bounded symmetric domain of E. Cartan, of complex dimension ab (Let us recall that $a + b = sq$). As before, if we take into account all the components in the representation (56) of ($\underline{\mathscr{F}}$), we are led to a g-fold product of the domain defined by (69)′, which is of complex dimension $\sum_{k=1}^{g} a_k b_k$.

It is remarkable that in none of the four cases discussed above, we arrive at the fourth type of E. Cartan's symmetric domains.

The results above may be formulated as

Theorem 6. *Any R-matrix in* ($\underline{\mathscr{F}}$) *satisfying the conditions* $R^2 = -E$, $(\mathsf{J}R) = (\mathsf{J}R)' > 0$ *is of the form* (56) *where the component matrices are of the form* (59) *with* $Z_0 = H + iG$ *belonging to one of the three types of E. Cartan's bounded symmetric domains mentioned above, the type being determined by* ($\underline{\mathscr{F}}$).

In each one of the four cases above, the set of such $R \in (\underline{\mathscr{F}})$ is non-empty; for example, $R = -\mathsf{J}$ is always in this set, since $-\mathsf{J}^2 = E_{hs^2}$ is **76**

positive symmetric. In case (iv), if $a_k b_k = 0$ for all k, then $R = -\mathsf{J}$ is the only R-matrix occurring in $(\underline{\mathscr{F}})$ with the normal form (56).

Let us define $\lambda = h$ in case $\mathscr{V} = \mathfrak{R}$, $\mathscr{G}$ or $\mathscr{P}$ and $\lambda = g$ in case $\mathscr{V}$ is a cyclic algebra carrying an involution of the second kind. From the form (56) of elements of $(\underline{\mathscr{F}})$, $R = [R_1, \ldots, R_\lambda]$ where each component $R_k (1 \leq k \leq \lambda)$ occurs with multiplicity μ equal to 1 in cases (i) and (iii) and equal to 2 or s in cases (ii) and (iv) respectively. We recall that to each $R_k (1 \leq k \leq \lambda)$ corresponds a Riemann matrix $\mathscr{P}_k$ under the correspondence $R_k = \left(\frac{\mathscr{P}_k}{\mathscr{P}_k}\right)^{-1} L_0 \left(\frac{\mathscr{P}_k}{\mathscr{P}_k}\right)$ where $L_0 = [-iE_\nu, iE_\nu]$, 2ν being the numbers of rows of R_k. Now hs_q^2 is an even integer, say $2n$, in all the four cases. Let us denote by L, the matrix $[-iE_n, iE_n]$. Then to the R-matrix R in $(\underline{\mathscr{F}})$ corresponds the n-rowed Riemann matrix $\mathscr{P}$ by means of the relation $R = \left(\frac{\mathscr{P}}{\mathscr{P}}\right)^{-1} L \left(\frac{\mathscr{P}}{\mathscr{P}}\right)$. For a suitable permutation matrix V, we have $V^{-1} L V = \underset{\mu\lambda}{L_0}$. From this, it is immediate that

$$\mathscr{P} = \begin{pmatrix} E_\mu \times \mathscr{P}_1 & 0 \ldots & 0 \\ 0 & E_\mu \times \mathscr{P}_2 \ldots & 0 \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ 0 & \ldots\ldots & E_\mu \times \mathscr{P}_\lambda \end{pmatrix} \tag{70}$$

is a Riemann matrix corresponding to R. Each $\mathscr{P}_k$ is a Riemann matrix of ν rows and 2ν columns with $\nu = \frac{q}{2}, q, 2q, sq$ in cases (i), (ii), (iii) and (iv) respectively. Further each $\mathscr{P}_k$ is of the form

$$\mathscr{P}_k = \left(i \frac{E_\nu + Z_k}{E_\nu - Z_k}, E_\nu \right) \tag{71}$$

77 where $Z_k = Z_k'$ and $E_\nu - \overline{Z}_k Z_k' > 0$. Let us denote by $\mathfrak{H}$, the set of $\mathscr{P}$ of the form (70) with $\mathscr{P}_k$ of the form (71), corresponding to all R-matrices in $(\underline{\mathscr{F}})$. As we saw, $\mathfrak{H}$ consists of at least of one point $\mathscr{P}$ of the form (70) with all $\mathscr{P}_k = (iE_\nu, E_\nu) (1 \leq k \leq \lambda)$ and consists exactly of this point when $a_k b_k = 0 (1 \leq k \leq \lambda)$.

We may now return to the problem of finding R-matrices R in $(\underline{\mathscr{F}})$ admitting $(\mathscr{M})$ as the *exact* algebra of commutators. For a given R-matrix R in $(\underline{\mathscr{F}})$, let us denote by $(\mathscr{R})$ the algebra of all real matrices

M commuting with R. Then clearly, $(\mathscr{R}) \supset (\underline{\mathscr{M}})$. If R were to have at least one rational commutator not in $(\mathscr{M})$, then the rank of $(\mathscr{R})$ over $\mathbb{R}$ will be strictly greater than hs^2 which is the rank of $(\underline{\mathscr{M}})$ over $\mathbb{R}$, or what is the same as the rank of $(\mathscr{M})$ over $\mathbb{Q}$. Thus our problem is to find out R-matrices R in $(\mathscr{F})$ for which the corresponding real commutator-algebra $(\mathscr{R})$ has rank exactly hs^2 over $\mathbb{R}$. The advantage in introducing $(\mathscr{R})$ is the following. Taking first the normal forms given in Theorem 5, the algebra $(\underline{\mathscr{F}})$ is the commutator-algebra of $(\underline{\mathscr{M}})$. Let C be a real non-singular matrix such that the elements of $C^{-1}(\underline{\mathscr{F}})C$ have precisely the normal form given by (56). Then $(\underline{\mathscr{F}})_1 = C^{-1}(\underline{\mathscr{F}})C$ is the commutator-algebra of $(\underline{\mathscr{M}})_1$. But the rank over $\mathbb{R}$ of $(\underline{\mathscr{M}})$ and $(\underline{\mathscr{M}})_1$ are the same. Thus, in connection with the problem mentioned at the beginning of this paragraph, we are free to look among the elements of $(\mathscr{F})_1$ itself, for R-matrices for which the corresponding algebra of all *real* commutators has rank exactly hs^2 over $\mathbb{R}$. By a "rational" commutator of a R-matrix in $(\underline{\mathscr{F}})_1$, we shall mean a commutator of the form $C^{-1}MC$ with rational M. The set of "rational" commutators is countable. We denote the algebra **78** $C^{-1}(\mathscr{M})C$ by $(\mathscr{M})_1$.

We know that the equation $RM = MR$ for a R-matrix R corresponds, in terms of the associated Riemann matrix $\mathscr{P}$, to the equation

$$\mathscr{P}M = K\mathscr{P} \tag{72}$$

where K is a complex matrix. Let then, for a $\mathscr{P} \in \mathfrak{H}$, the equation (72) hold, for a real M. Splitting up M and K as (M_{kl}) and (K_{kl}) corresponding to the decomposition (70) of $\mathscr{P}$, we obtain

$$(E_\mu \times \mathscr{P}_k)M_{kl} = K_{kl}(E_\mu \times \mathscr{P}_\ell) \tag{73}$$

for $l \leq k$, $1 \leq \lambda$. We break up M_{kl} and K_{kl} respectively into 2ν-rowed and ν-rowed square matrices corresponding to the decomposition of $E_\mu \times \mathscr{P}_k$ and $E_\mu \times \mathscr{P}_1$ and denoting a typical block by M_0 and K_0 respectively, we have, from (73)

$$\mathscr{P}_k M_0 = K_0 \mathscr{P}_1 \tag{74}$$

with complex K_0. Now $\mathscr{P}_k$ and $\mathscr{P}_1$ are of the form (71); splitting up

M_0 as $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ with ν-rowed square A, we have, from (74),

$$i \cdot \frac{E_\nu + Z_k}{E_\nu - Z_k} A + C = K_0 \quad i \cdot \frac{E_\nu + Z_1}{E_\nu - Z_1}$$
$$i \cdot \frac{E_\nu + Z_k}{E_\nu - Z_k} B + D = K_0$$

Elimination of K_0 leads to the equations (for $1 \leq k, l \leq \lambda$)

$$i(E_\nu + Z_k)A(E_\nu - Z_1) + (E_\nu - Z_k)C(E_\nu - Z_1) + (E_\nu + Z_k)B(E_\nu + Z_1) - i(E_\nu - Z_k)D(E_\nu + Z_1) = 0. \quad (75)$$

Conditions (75) are necessary and sufficient for $\mathscr{P} \in \mathfrak{H}$ to have M as a multiplier. Referred to as the "singular relations they have been studied thoroughly by G. Humbert [10] for $n = 2$.

79 For any $M \in (\mathscr{M})_1$, we know that equations (75) hold *identically* for $\mathscr{P} \in \mathfrak{H}$. If not $\mathscr{P} \in \mathfrak{H}$ admits a "rational" multiplier M_1 (i.e. if M_1 is a "rational" commutator of the associated R-matrix), then $\mathscr{P}$ necessarily belongs to the quadratic surface defined in $\mathfrak{H}$ by conditions (75) corresponding to this M_1. (Of course, if it turns out that every $\mathscr{P} \in \mathfrak{H}$ admits this M_1 as a multiplier, then this quadratic surface coincides with the whole of $\mathfrak{H}$). The number of such surfaces, for $M_1 \notin (\mathscr{M})_1$, is, at any rate, countable. The complement of the union of these countably many surfaces may be seen to be dense in $\mathfrak{H}$.

Let us suppose that for *all* $\mathscr{P} \in \mathfrak{H}$, a real matrix $M = (M_{kl})$ is a multiplier. Then, with the same notation as above, conditions (75) are valid with arbitrary Z_k, Z_l in the "generalized unit disc" of degree ν (such that $\mathscr{P} \in \mathfrak{H}$). In particular, taking $Z_k = 0 = Z_1$, $\mathscr{P} \in \mathfrak{H}$ and then (75) gives $iA + C + B - iD = 0$ i.e. $A = D$, $B = -C$. Thus $M_0 = \left(\begin{smallmatrix} A & B \\ -B & A \end{smallmatrix}\right)$. Now the quadratic terms in (75) cancel out and we are left with the equation

$$2iZ_kA - 2iAZ_1 + 2Z_kB + 2BZ_1 = 0$$

Setting $F = A + \underline{iB}$, we have then

$$Z_k\overline{F} = FZ_1 \quad (76)$$

We split our further considerations into four parts according as $\mathscr{V} = \mathfrak{R}$, $\mathscr{G}$, $\mathscr{P}$ or a cyclic algebra. First, we take up the case $\underline{\mathscr{V} = \mathfrak{R} \text{ or } \mathscr{G}}$. Here

$\mu = 1$ or 2 respectively. Further, Z_k, Z_l are arbitrary elements of the "generalized unit disc" of degree ν. Taking $Z_k = Z_l = tE_\nu (0 < t < 1)$ in (76), we see that $F = \overline{F}$ or $B = 0$. Now $Z_k F = F Z_l$ and since Z_k, Z_l **80** are arbitrary elements of the "generalized unit disc", we can show that for $k \neq 1$, we have $A = 0$ and for $k = 1$, $A = \alpha E_\nu$ with arbitrary α in $\mathbb{R}$. Thus when $\mathscr{V} = \mathfrak{H}$, we see that $M_{kl} = 0$ for $k \neq 1$ and $M_{kk} = \alpha_k E_{2\nu}$; with arbitrary real α. For $\mathscr{V} = \mathscr{G}$, again $M_{kl} = 0$ for $k \neq 1$, while $M_{kk} = \begin{pmatrix} \alpha_k E_{2\nu} & k\beta_k E_{2\nu} \\ \gamma_k E_{2\nu} & \delta_k E_{2\nu} \end{pmatrix}$ with arbitrary α_k, β_k, γ_k, δ_k in $\mathbb{R}$. Thus the rank over $\mathbb{R}$ of the algebra of real matrices which are multipliers for *every* $\mathscr{P} \in \mathfrak{H}$ is h or 4th according as $\mathscr{V} = \mathfrak{R}$ or $\mathscr{G}$. But the rank of $(\underline{\mathscr{M}})$ over $\mathbb{R}$ is the same in both these cases. Thus (75) does not hold identically for $\mathscr{P} \in \mathfrak{H}$, if M is a "rational" multiplier not in $(\mathscr{M})_1$. In fact, if $\mathscr{P}$ does not belong to the countably many quadratic surfaces in $\mathfrak{H}$ corresponding to such "rational" multipliers not in $(\mathscr{M})_1$, then it has $(\mathscr{M})_1$ as its exact algebra of multipliers. Thus *our problem of finding a R-matrix with* $(\mathscr{M})$ *as exact commutator-algebra admits of a solution in these two cases.*

Example. If $q = 1$ and $\mathscr{V} = \mathbb{Q}$, then any point $\mathscr{P} = (\tau, 1) \in \mathfrak{H}$ (with $\tau = \alpha + \beta\sqrt{d}$, $\alpha, \beta, d (< 0)$ in $\mathbb{Q}$) admits all the elements of $\mathscr{F} = \mathbb{Q}(\sqrt{d})$ as multipliers. Clearly $\mathscr{F}$ contains $\mathbb{Q}$ properly. Such points τ are countably many and constitute a dense set in the complex upper half-plane; the complement of this set also is dense in the upper half-plane.

We now take up for consideration the cases (iii) and (iv). In these two cases, $\lambda = h$ or g, $\mu = 1$ or s, $\nu = 2q$ or sq respectively. Further, for $1 \leq k \leq \lambda$,

$$\mathscr{P}_k = \left(i\frac{E_\nu + Z_k}{E_\nu - Z_k}, E_\nu \right) \text{ with } Z_k = \begin{pmatrix} 0 & W_k \\ W_k' & 0 \end{pmatrix}$$

Further in case (iii) $W_k = -W_k'$ is a q-rowed complex matrix satisfying **81** $E_q - \overline{W}_k W_k' > 0$ while, in case (iv), W_k is a complex matrix of a_k rows and b_k columns such that $E_{a_k} - \overline{W}_k W_k' > 0$ and $a_k + b_k = sq$. If, in case (iii), $q = 1$, then $W_k = 0$; in case (iv), if $a_k b_k = 0$, then Z_k is to be taken just as the zero matrix of sq rows and columns.

We start from condition (76) and splitting up F as $\begin{pmatrix} F_1 & F_2 \\ F_3 & F_4 \end{pmatrix}$ with square F_1 having the same number of rows as W_1, we may rewrite (76)

as follows, namely,

$$\begin{aligned} W_k\overline{F}_3 &= F_2W_1' \\ W_k\overline{F}_4 &= F_1W_1 \\ W_k'\overline{F}_1 &= F_4W_1' \\ W_k'\overline{F}_2 &= F_3W_1 \end{aligned} \tag{76}'$$

Let now $\mathscr{V} = \mathscr{P}$ *and* $q \geq 3$. (The situation when $\mathscr{V} = \mathscr{P}$ and $q = 1$ or 2 is more complicated and will be dealt with later on). We consider first, for $k \neq 1$, the equation $W_k\overline{F}_3 = F_2W_1'$ in (76)′. Let $W_k = (u_{\alpha\beta})$, $F_3 = (a_{\gamma\delta})$, $F_2 = (b_{\rho\zeta})$, $W_1 = (v_{\kappa\omega})$. Comparing the $(\kappa, \delta)^{\text{th}}$ element on both sides of the matrix equation, we have

$$\sum_{\omega=1}^{q} u_{\kappa\omega}\overline{a}_{\omega\delta} = \sum_{\zeta=1}^{q} b_{\kappa\zeta}v_{\delta\zeta} \tag{77}$$

Here, except for the relations $u_{\kappa\kappa} = 0$, $v_{\kappa\zeta} = -u_{\zeta\kappa}$ and similar relations
82 for the elements of W_1, we may regard the elements $v_{\kappa\omega}$ of W_k and the elements $v_{\zeta\delta}$ of W_1 as independent variables. As a consequence, it can be shown that $F_2 = 0$, $F_3 = 0$, for $k \neq 1$. Similarly using the equation $W_k\overline{F}_4 = -F_1W_1'$ in (76)′, it can be proved that $F_1 = 0$, $F_4 = 0$ for $k \neq 1$. Thus, for $k \neq 1$, the matrix F occurring in (76) is 0. We may now take up the discussion of (76) for $\underline{k = 1}$. Then we have, in particular, from (76)′

$$W_k\overline{F}_3 = F_2W_k' \tag{78}$$

$$W_k\overline{F}_4 = -F_1W_k' \tag{79}$$

Using the same notation as in (77), we obtain from (78) that

$$\sum_{\omega=1}^{q} u_{\kappa\omega}\overline{a}_{\omega\delta} = \sum_{\zeta=1}^{q} b_{\kappa\zeta}u_{\delta\zeta} \tag{80}$$

We now proceed to show that, for $\varepsilon \neq \delta$, $a_{\varepsilon\delta} = 0$. *Since* $\underline{\nu = q \geq 3}$, there exists $\eta \neq \varepsilon, \delta$ such that $u_{\eta\varepsilon} \not\equiv 0$ and then with $\kappa = \eta$, (80) becomes

$$\sum_{\omega=1}^{q} u_{\eta\omega}\overline{a}_{\omega\delta} - \sum_{\zeta=1}^{q} b_{\eta\zeta}u_{\delta\zeta} = 0 \tag{81}$$

But the left hand side of (81) is a linear form in the variables $u_{\alpha\beta}$ with the coefficient of $u_{\eta\varepsilon}$ equal to $\overline{a}_{\varepsilon\delta}$. Hence $a_{\varepsilon\delta} = 0$. Similarly, we can show that $b_{\eta\zeta} = 0$ for $\eta \neq \zeta$. Thus F_2, F_3 are diagonal matrices; using (79), it would follow again that F_1, F_4 are also diagonal. Now, from (81),

$$u_{\eta\delta}\left(\overline{a}_{\delta\delta} + b_{\eta\eta}\right) + \sum_{\substack{\omega=1 \\ \omega\neq\delta}}^{q} u_{\eta\omega}\overline{a}_{\omega\delta} - \sum_{\substack{\zeta=1 \\ \zeta\neq\eta}}^{q} b_{\eta\zeta}u_{\delta\zeta} = 0$$

By the same arguments as above, we have

$$\overline{a}_{\delta\delta} = -b_{\eta\eta} \tag{82}$$

Analogous to (81), we have $\sum_{\omega=1}^{q} u_{\eta\omega}\overline{a}_{\omega\varepsilon} - \sum_{\zeta=1}^{q} b_{\eta\zeta}u_{\varepsilon\zeta} = 0$. From this we **83**
may deduce as above that

$$\overline{a}_{\varepsilon\varepsilon} = -b_{\eta\eta} \tag{83}$$

From (82) and (83), it follows that $F_3 = a_{11}E_q$ and now from (78) we deduce that $F_2 = -\overline{F}_3$. In a similar manner, we can use (79) to show that $F_4 = \overline{F}_1 = \overline{x}E_q$ where x is a complex number. Thus finally we see that, for $k = 1$, the matrix F occurring in (76) is of the form $\left(\begin{smallmatrix} x & y \\ -\overline{y} & \overline{x} \end{smallmatrix}\right) \times E_q$ where x, y are arbitrary complex. Referring to (72), if M is a real matrix which is a multiplier for *all* $\mathscr{P} \in \mathfrak{H}$, then $M = [M_{11}, \ldots, M_{kk}, \ldots, M_{hh}]$ where each M_{kk} is a real matrix with 4 independent real parameters. Thus the rank over $\mathbb{R}$ of the algebra of all real matrices commuting with all the R-matrices in $(\mathscr{F})$ is $4h$, which is precisely the rank over $\mathbb{R}$ of $(\mathscr{M})$. We may conclude, as before, that for $\mathscr{V} = \mathscr{P}$ and $q \geq 3$, *there exist R-matrices in* $(\mathscr{F})$ *admitting* $(\mathscr{M})$ *as the exact commutator-algebra.*

We now take up case (iv) when $\mathscr{V}$ is a cyclic algebra with an involution of the second kind and *assume* further that $qs \geq 3$ and *not all* $a_k b_k$ *are equal to zero.* We may, without loss of generality, suppose that for $1 \leq k \leq r \leq g$, we have $a_k b_k > 0$. Observe that $a_k b_k > 0$, $qs \geq 3$ together imply that at least one of a_k, b_k is greater than 1. We go back to consider equation (76). If $k > r$ and $1 \leq r$, then we have $FZ_1 = 0$ for all Z_1 and consequently $F = 0$. Similarly, if $1 > r$ and $k \leq r$, we have

again $F = 0$ in (76). Let us now suppose that $1 \leq k$, $1 \leq r$. From (76)′, we may deduce a relation analogous to (77). But now the elements of
84 W_k are independent complex variables which are again independent of the elements of W_1 (for $1 \neq k$). Further, at least one of a_k, b_k is greater than or equal to 2 and similarly for a_1, b_1. It is easy to deduce as before that for $k \neq 1$, $1 \leq k$, $1 \leq r$, we have $F = 0$, while for $1 \leq k = 1 \leq r$, we see that $F = \left(\begin{smallmatrix} x & 0 \\ 0 & \overline{x} \end{smallmatrix}\right) \times E_\nu$ where x is arbitrary complex. Thus, referring to (73), M_{kk} is a real matrix with $2s^2$ real parameters. We may then conclude that any real matrix M which is a multiplier for all Riemann matrices $\mathscr{P} \in \mathfrak{H}$ is necessarily of the form

$$M = [M_{11}, \ldots, M_{rr}, N] \tag{84}$$

where $M_{11}, \ldots, M_{rr}$ are real matrices with $2s^2$ independent real parameters and N is a $2(g-r)s^2q$-rowed real square matrix.

If $r = g$, in other words, $a_k b_k > 0$ for $1 \leq k \leq g$ and $qs \geq 3$, then the rank over $\mathbb{R}$ of the algebra of all such matrices R is $2gs^2 = hs^2$ which is precisely the rank over $\mathbb{R}$ of $(\mathscr{M})$. Thus in the case when $\mathscr{V}$ is a cyclic algebra with an involution of the second kind and further $qs \geq 3$, $a_k b_k > 0 (1 \leq k \leq g)$, we see that *there exist R-matrices with* $(\mathscr{M})$ *as the complete commutator-algebra.*

If $1 \leq r < g$, we know nothing about the nature of the matrix N appearing in (84). Therefore, before we proceed to discuss the case when $qs \geq 3$ and $1 \leq r < g$, we need to prove

Lemma 3. *Let $\mathscr{L}$ be an algebraic numberfield of degree g over $\mathbb{Q}$, with $\omega_1, \ldots, \omega_g$ as a basis over $\mathbb{Q}$ and let Ω stand for the g-rowed square matrix $(\omega_k^{(l)})$ $(1 \leq k, l \leq h)$. Further, let Q be a g-rowed square matrix of the form $\left(\begin{smallmatrix} a & * \\ 0 & B \end{smallmatrix}\right)$ with a complex number a and let $\Omega Q \Omega^{-1}$ be rational. Then, necessarily $a \in \mathscr{L}$ and furthermore, $Q = [a^{(1)}, \ldots, a^{(g)}]$.*

85 *Proof.* Let $\Omega Q \Omega^{-1} = (p_{kl})(1 \leq k, l \leq g)$. Then $\Omega Q = (p_{kl})\Omega$ and, in particular, we have $\omega_k a = \sum_{1=1}^{g} p_{kl}\omega_1 (p_{kl} \in \mathbb{Q})$. Hence $a = \sum_{1=1}^{g} p_{11}\frac{\omega_1}{\omega_1} \in \mathscr{L}$ (since $\omega_1 \neq 0$) and $a^{(1)} = a, a^{(2)}, \ldots, a^{(g)}$ are its conjugates over $\mathbb{Q}$. But we know that $\Omega[a^{(1)}, \ldots, a^{(g)}] = (p_{kl})\Omega$ and therefore $Q = [a^{(1)}, \ldots, a^{(g)}]$. □

Remark. We shall use, in the sequel, a generalization of Lemma 3 (the proof of which is exactly on the same lines) namely, the following.

Let $d \geq 1$ be a rational integer and $\mathscr{L}$, Ω as in the hypothesis of Lemma 3. Let $Q = \left(\begin{smallmatrix} H & * \\ Q & * \end{smallmatrix}\right)$ with a d-rowed complex square matrix H and let $(\Omega \times E_d)Q(\Omega \times E_d)^{-1}$ be rational. Then necessarily, the elements of H are in $\mathscr{Z}$ and further, $Q = [H^{(1)}, \ldots, H^{(g)}]$.

We may proceed now to discuss case (iv) with the assumption that $qs \geq 3$, $1 \leq r < g$. In order that the application of the above-mentioned generalization of Lemma 3 be feasible, we do not go right up to the eventual normal form (56) of $(\underline{\mathscr{F}})$ but we stop short somewhat earlier. So let us start de novo. From the representation $\delta \to D_0$ of $\mathscr{V}$ over $\mathfrak{R}$ given on p. 37, we first get a representation $\delta \to D_1$ of $\mathscr{V}$ over $\mathscr{L}$ as follows; namely, if $(1, \sqrt{c})$ is a basis of $\mathfrak{R}$ over $\mathscr{Z}$, then denoting the matrix $\left(\begin{smallmatrix} 1 & 1 \\ \sqrt{c} & -\sqrt{c} \end{smallmatrix}\right)$ by Ω_1, we define D_1 by $D_1 = (\Omega_1 \times E_{s^2})[D_0, \overline{D}_0](\Omega_1 \times E_{s^2})^{-1}$. Now, we can get from this a rational representation $\delta \to \underline{D}$ of $\mathscr{V}$ by the prescription

$$\delta \to \underline{D} = C_1 \begin{bmatrix} D_1^{(1)} & & \\ & \ddots & \\ & & D_1^{(g)} \\ q & & q \end{bmatrix} C_1^{-1}$$

where $C_1 = \Omega_1^* \times E_{2s^2q}$, $\Omega_1^* = (\delta_k^{(1)})$, $\delta_1, \ldots, \delta_g$ is a basis of $\mathscr{L}$ over $\mathbb{Q}$ **86**
and $D_1^{(1)}, \ldots, D_1^{(g)}$ are the conjugates of D_1 over $\mathbb{Q}$. Thus the elements of the algebra $(\mathscr{M})_2 = C_1^{-1}(\mathscr{M})C_1$ are of the form $[D_1^{(1)}, \ldots, D_1^{(g)}]$ where D_1 is a $2s^2q$-rowed square matrix with elements in $\mathscr{L}$. Defining the algebra $(\underline{\mathscr{F}})_2$ by $(\underline{\mathscr{F}})_2 = C_1^{-1}(\underline{\mathscr{F}})C_1$, we shall look for R-matrices in $(\underline{\mathscr{F}})_2$ with the required properties. Applying to $(\underline{\mathscr{F}})_2$ the procedure given earlier to reduce $(\underline{\mathscr{F}})$ to the normal form (56), we remark that this merely involves going over to the representation $C_2^{-1}(\underline{\mathscr{F}})_2 C_2$ (where $C_2 = [C_{2,1}, \ldots, C_{2,g}]$ with $2s^2q$-rowed real square matrices $C_{2,k}$). Let M_0 be a *rational* matrix commuting with all R-matrices in $(\underline{\mathscr{F}})$. Then $M = C_2^{-1}C_1^{-1}M_0C_1C_2$ commutes with all the corresponding R-matrices in $C_2^{-1}(\underline{\mathscr{F}})_2C_2$. Since $r \geq 1$, it follows, by using the same arguments as for the case $r = g$ above, that M and hence $M_2 = C_2MC_2^{-1}$ is of the form (84). As yet we know nothing about the number of parameters involved in N. But now $M_0 = C_1M_2C_1^{-1}$ is rational and appealing to our

Remark on p. (85), we conclude that M_{11} has elements in $\mathscr{Z}$ and further M_2 itself is of the form

$$M_2 = [M_{11}^{(1)}, \ldots, M_{11}^{(g)}] \tag{85}$$

If we take M_0 to be real instead of being rational, and further if M_0 commutes with all the R-matrices in $(\underline{\mathscr{F}})$ we see, by arguments as in the case $r = g$, that $C_1 M_0 C_1^{-1}$ is of the form (84) again, with each $M_{kk}(1 \leq k \leq r)$ having $2s^2$ independent real parameters. Now such M_{11} constitute precisely the linear closure of the matrices $M_{11}^{(1)}$ occur-
87 ring in (85) with elements in $\mathscr{Z}$. Thus the matrices $M_{11}^{(1)}$ in (85) form an algebra of rank $2s^2$ over $\mathscr{Z}$. Let indeed then $F_1, \ldots, F_{2s^2}$ be a basis of this algebra so that every such $M_{11}^{(1)} = \sum_{k=1}^{2s^2} x_k F_k$ (with $x_k \in \mathscr{Z}$). Hence, in (85), $M_{11}^{(1)} = \sum_{k=1}^{2s^2} x_k^{(1)} F_k^{(1)}$. This enables us to conclude that if M_0 is a real commutator of all R-matrices in $(\underline{\mathscr{F}})$, then, by virtue of M_0 lying in the linear closure of rational commutators of the same kind, $C_1 M_0 C_1^{-1} = [M_{11}, \ldots, M_{gg}]$ where $M_{kk} = \sum_{l=1}^{2s^2} x_l F_l^{(k)}$ and $x_1, \ldots, x_{2s^2}$ are arbitrary real numbers. In other words, the rank of the algebra of real commutators of *all* R-matrices in $(\mathscr{F})$ is $2gs^2 = hs^2$. Thus *for* $qs \geq 3$, $1 \leq r \leq g$, *there do exist R-matrices with* $(\mathscr{M})$ *as the complete commutator algebra.*

We shall now prove that for $qs \geq 2$ and $r = 0$ (i.e. $a_k b_k = 0$ for all k), *there cannot exist R-matrices with* $(\mathscr{M})$ *as the complete commutator-algebra.* Since $a_k b_k = 0$ for $1 \leq k \leq g$, the only R-matrix in $(\underline{\mathscr{F}})_1 = C^{-1}(\underline{\mathscr{F}})C$ (referring to the notation on p. 56) is $-\mathsf{J} = [\underbrace{-\mathsf{J}_0, \ldots, -\mathsf{J}_0}_{g \text{ times}}]$. Now the matrices P_k occurring in case (iv) in (56) are all $\pm E_{sq}$ and therefore all the matrices in $(\underline{\mathscr{F}})_1$ commute with $-\mathsf{J}$. Thus all elements of $(\underline{\mathscr{F}})$ commute with the R-matrix $R = -C\mathsf{J}C^{-1}$; in particular, every element of $(\mathscr{F})$ commutes with R. If now R were to have $(\mathscr{M})$ as its exact commutator algebra, then $(\mathscr{F}) \subset (\mathscr{M})$, necessarily. But, by Proposition 6, $(\mathscr{F}) \cap (\mathscr{M}) = (\mathfrak{R})$. Hence $(\mathscr{F}) = (\mathfrak{R})$. Now, if $qs \geq 2$, then either $q > 1$ or $s > 1$. If $q > 1$, then $(\mathscr{F})$ is the q-rowed matrix-algebra over
88 the commutator algebra $(\mathscr{V})^*$ of $(\mathscr{V})$ and therefore it is not commutative.

But then $(\mathscr{F}) = (\mathfrak{R})$ gives a contradiction. Again, if $q = 1$ and $s > 1$, then $(\mathscr{V})$ is non-commutative and so is $(\mathscr{F}) = (\mathscr{V})^*$, which contradicts $(\mathscr{F}) = (\mathfrak{R})$. Thus our assertion above is proved.

The exceptional cases which remain to be considered are the following, namely a) $\mathscr{V} = \mathscr{P}$, $q = 1$ or 2 and b) $\mathscr{V}$, a cyclic algebra with an involution of the second kind with $qs = 1$ or with $qs = 2$ and not all $a_k b_k$ equal to zero. We shall slightly reformulate our problem of finding R-matrices in $(\underline{\mathscr{F}})$ for which 1) $AR = S = S' > 0$ where $A = \underset{q}{G} T_0$ with $T_0 = -\widetilde{T}_0$ in $(\mathscr{F})$, 2) $R^2 = -E$ and 3) $(\mathscr{M})$ is the complete commutator-algebra. Let us set $N = T_0 R$. Then barring the last condition, in terms of N, these conditions are merely that 1) $N \in (\underline{\mathscr{F}})$ 2) $N = \underset{q}{G^{-1}} N' \underset{q}{G} = L^{-1} \underset{q}{F^{-1}} \underset{q}{F} L = (\underset{q}{F^{-1}} N' \underset{q}{F}) L^{-1} L = \widetilde{N}$ and 3) $(T_0^{-1} N)^2 = -E$. On the other hand, by Lemma 2, $S = \underset{q}{G} N > 0$ and $\underset{q}{G} > 0$ together imply that all the eigenvalues of N are real and positive. Thus our problem reduces to finding $N \in (\underline{\mathscr{F}})$ for which

$$N = \widetilde{N}, T_0^{-1} N \; T_0^{-1} N = -E; \text{ the eigenvalues of } N \text{ are real and positive .} \tag{86}$$

We shall first take up the case when $\underline{\mathscr{V} = \mathscr{P}, q = 1}$. Choosing for $(\mathscr{M})$, the 4-rowed representation of the opposite algebra $\mathscr{P}^*$ of $\mathscr{P}$ without loss of generality, we may suppose that $(\mathscr{F})$ is the 4-rowed representation $\delta \to D$ of $\mathscr{P}$ over $\mathfrak{R}$, given on p. 46. We observe that the involution $T \to \widetilde{T}$ in $(\mathscr{F})$ is a positive involution since $\sigma(T\widetilde{T}) = \sigma(T \underset{q}{F^{-1}} T' \underset{q}{F})$ is a positive definite form over the centre $\mathfrak{R}$ in view of F being positive definite. But now we know that the abstract totally **89**
definite quaternion algebra $\mathscr{P}$ has a unique positive involution, viz. $\delta = x + yi + zj + tk \to \widetilde{\delta} = x - yi - zj - tk$. Thus, for $N \in (\underline{\mathscr{F}})$, $N = \widetilde{N}$ implies that N is in the center of $(\underline{\mathscr{F}})$. This gives $R = T_0^{-1} N = N T_0^{-1}$ i.e. $T_0 R = N = R T_0$. Now suppose that there exists a R-matrix R in $(\underline{\mathscr{F}})$ for which $(\mathscr{M})$ is the exact commutator-algebra. Then T_0 being a rational commutator of R, $T_0 \in (\mathscr{M})$. Since $T_0 \in (\mathscr{F})$ too, we have $T_0 \in (\mathscr{F}) \cap (\mathscr{M}) = (\mathfrak{R})$. This gives us $T_0 = \widetilde{T}_0$ but the we have a contradiction to $T_0 = -\widetilde{T}_0$ from which we started. We may thus conclude that in the case $\underline{\mathscr{V} = \mathscr{P}, q = 1}$, *there cannot exist R-matrices with* $(\mathscr{M})$

as the exact commutator-algebra.

Next we consider the case when $\underline{\mathscr{V} = \mathscr{P}}$ and $\underline{q = 2}$. By choosing a suitable representation $(\mathscr{P})$ of $\mathscr{P}$, we can suppose, without loss of generality, that for the elements δ of the commutator-algebra $(\widehat{\mathscr{P}})$ of $(\mathscr{P})$, we already have the representation $\delta \to [D^{(1)}, \ldots, D^{(h)}]$ over the centre $\mathfrak{R}$ and its conjugates over $\mathbb{Q}$, as indicated on p. 46. Now $T_0 = \left(\begin{smallmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{smallmatrix}\right) = -\widetilde{T}_0$ with $\alpha_1, \beta_1, \gamma_1, \delta_1$ in $(\widehat{\mathscr{P}})$. We first remark that there exists a 2-rowed non-singular matrix W with elements in $(\widehat{\mathscr{P}})$ such that $\widetilde{W}T_0W = \left(\begin{smallmatrix} \alpha_2 & 0 \\ 0 & \beta_2 \end{smallmatrix}\right)$ with $\alpha_2 = -\widetilde{\alpha}_2, \beta_2 = -\widetilde{\beta}_2$ in $(\widehat{\beta})$. If now for some p in $(\mathfrak{R})$, we have $\beta_2 = p\alpha_2$, then we can easily find $\lambda \neq 0$ in $(\widehat{\mathscr{P}})$ such that $\widetilde{\lambda}\beta_2\lambda$ does not commute with α_2. Therefore, choosing, for example, $W\left(\begin{smallmatrix} 1 & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ instead of W, we could suppose that for no element p in $(\mathfrak{R})$ do we have $\beta_2 = p\alpha_2$. The matrix $N \in (\underline{\mathscr{F}})$ has the properties mentioned
90 in (86). Now it is trivial to see that $\widetilde{W}NW$ is again symmetric under the involution in $(\underline{\mathscr{F}})$. Moreover, from (86), we have, in view of Lemma 2, that $\underset{2}{F}N$ is symmetric and positive-definite. Hence $W'\underset{2}{F}NW = \underset{2}{F}\widetilde{W}NW$ is again symmetric and positive-definite. By Lemma 2 again, $\widetilde{W}NW$ has its eigen-values real and positive. Thus taking $W^{-1}RW$, $\widetilde{W}NW$ and $\widetilde{W}T_0W$ instead of R, N and T_0 respectively we could suppose from the beginning that $T_0^{-1} = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ with $\alpha = -\widetilde{\alpha}, \beta = -\widetilde{\beta}$ in $(\widehat{\mathscr{P}})$ and $N = \left(\begin{smallmatrix} x & \omega \\ \widetilde{\omega} & y \end{smallmatrix}\right)$ has the properties mentioned in (86). Denoting by $(\underline{\mathfrak{R}})$ the centre of $(\underline{\widehat{\mathscr{P}}})$, we see that

$$\begin{aligned} &x = [\underset{4}{x_1}, \ldots, \underset{4}{x_h}] > 0, y = [\underset{4}{y_1}, \ldots, \underset{4}{y_h}] > 0 \text{ are in } (\underline{\mathfrak{R}}) \\ &\omega = \widetilde{\omega} \in (\underline{\widehat{\mathscr{P}}}), xy - \omega\widetilde{\omega} > 0. \end{aligned} \tag{87}$$

(The last assertion in (87) is a consequence of the relation

$$N = \begin{pmatrix} 1 & 0 \\ x^{-1}\widetilde{\omega} & 1 \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & y - x^{-1}\widetilde{\omega}\omega \end{pmatrix}\begin{pmatrix} 1 & x^{-1}\omega \\ 0 & 1 \end{pmatrix}.$$

Now $R = T_0^{-1}N = \left(\begin{smallmatrix} \xi & \eta \\ \zeta & \tau \end{smallmatrix}\right)$ where $\xi = x\alpha, \eta = \alpha\omega, \zeta = \beta\widetilde{\omega}$ and $\tau = y\beta$. The condition $R^2 = -E$ may be written as

$$\begin{aligned} -cx^2 + \alpha\omega\beta\widetilde{\omega} = -1, cx\omega = y\alpha\omega\beta \\ \beta\widetilde{\omega}\alpha\omega - dy^2 = -1, dy\widetilde{\omega} = \alpha\beta\widetilde{\omega}\alpha \end{aligned} \tag{88}$$

where $\alpha^2 = -\alpha\widetilde{\alpha} = -c$, $\beta^2 = -\beta\widetilde{\beta} = -d$ with $c = [\underset{4}{c_1}, \ldots, \underset{4}{c_h}] > 0$, $d = [\underset{4}{d_1}, \ldots, \underset{4}{d_h}] > 0$ in $(\mathfrak{R})$. Writing $x = py$, with $p \in (\mathfrak{R})$, we obtain from (88),

$$c(x^2 - p\omega\widetilde{\omega}) = 1 = d\left(y^2 - \frac{\omega\widetilde{\omega}}{p}\right)$$

leading to $p^2 = dc^{-1}$. Thus $p = xy^{-1}$ is the positive square root of dc^{-1}; **91**
i.e. $p_k = \left|\sqrt{\dfrac{d^{(k)}}{c^{(k)}}}\right|$. Our problem on R-matrices now reduces to finding $x > 0$ in $(\underline{\mathfrak{R}})$ and $\omega \in (\widehat{\mathscr{P}})$ for which

$$\alpha\omega\beta = cp\omega \tag{89}$$

$$cx^2 - cp\omega\widetilde{\omega} = 1 \tag{90}$$

$$p^{-1}x^2 - \widetilde{\omega}\omega > 0$$

As a particular solution of (89), we have $\omega_0 = p\alpha - \beta$ (observe that $\omega_0 \neq 0$). The most general solution of (89) is given by $\omega = t\omega_0$ where $t \in (\widehat{\mathscr{P}})$ and $t\alpha = \alpha t$. Clearly $t = u + v\alpha$ with $u = [\underset{4}{u_1}, \ldots, \underset{4}{u_h}]$, $v = [\underset{4}{v_1}, \ldots, \underset{4}{v_h}]$ in $(\underline{\mathfrak{R}})$. Now, the first condition in (90) may be written as

$$cx^2 - cp\omega_0\widetilde{\omega}_0(u^2 + cv^2) = 1 \tag{90}'$$

Equation (90)′ defines a "two-sheeted hyperboloid" in the x, u, v-space; the $2h$ components of u and v are independent real parameters while the h components of x are linearly independent of the components of u, v although quadratically related to them. We finally arrive at the following parameterization for the R-matrix R, namely

$$R = \begin{pmatrix} py\alpha & \alpha(u + v\alpha)\omega_0 \\ \beta\widetilde{\omega}_0(u - v\alpha) & y\beta \end{pmatrix} \tag{91}$$

where $cp^2y^2 - cp\omega_0\widetilde{\omega}_0(u^2 + cv^2) = 1$.

Let $\gamma_1, \ldots, \gamma_h$ be a basis of $\mathfrak{R}$ over $\mathbb{Q}$ and let $\Omega = (\gamma_k^{(1)})$ with $1 \leq k,\ 1 \leq h$. For $\delta \in (\widehat{\mathscr{P}})$, we took the rational representation $(\Omega \times E_4)[D^{(1)}, \ldots, D^{(h)}](\Omega \times E_4)^{-1}$. Let, under this representation, $\alpha \to (\Omega \times$

$E_4)[A^{(1)}, \ldots, A^{(h)}](\Omega\times E_4)^{-1}$ and $\beta \to (\Omega\times E_4)[B^{(1)}, \ldots, B^{(h)}](\Omega\times E_4)^{-1}$. **92**
It is trivial to verify that $R = (\Omega \times E_8)[R_1, \ldots, R_h](\Omega \times E_8)^{-1}$ where

$$R_k = \begin{pmatrix} p_k y_k A^{(k)} & A^{(k)}(u_k E_4 + v_k A^{(k)})(p_k A^{(k)} - B^{(k)}) \\ B^{(k)}(p_k A^{(k)} - B^{(k)})(v_k A^{(k)} - u_k E_4) & y_k B^{(k)} \end{pmatrix}$$

for $1 \leq k \leq h$. Let now M_0 be any $8h$-rowed rational matrix commuting will all R-matrices in ($\underline{\mathscr{F}}$). Then $M = (\Omega \times E_8)^{-1} M_0 (\Omega \times E_8)$ has to commute with $[R_1, \ldots, R_h]$ and moreover $(\Omega \times E_8) M (\Omega \times E_8)^{-1}$ has to be rational. From the mutual independence of the parameters u_k, v_k, y_k and u_1, v_1, y_1 (for $k \neq 1$), it is clear that $M = [M_1, \ldots, M_h]$ and further by our Lemma, M_1 has elements in $\mathfrak{R}$ while $M_k = M_1^{(k)}$ for $1 \leq k \leq h$. In addition M_k commutes with R_k. We proceed to determine the structure of M_1, writing $M_1 = \left(\begin{smallmatrix} \rho & \kappa \\ \mu & \nu \end{smallmatrix}\right)$ with 4-rowed square matrices with elements in $\mathfrak{R}$. For the sake of brevity in notation, let us for the present, agree to understand by α, β the corresponding matrices $A^{(1)}$, $B^{(1)}$ and further let us omit the subscript in p_1, y_1, u_1, v_1. Then we see that M_1 has to commute necessarily with the matrix $\left(\begin{smallmatrix} py\alpha & \alpha(u+v\alpha) & \omega_0 \\ \beta\omega_0(v\alpha - u) & & y\beta \end{smallmatrix}\right)$. Equivalently M_1 has to commute with $\left(\begin{smallmatrix} p\alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$,

$$\begin{pmatrix} 0 & \alpha\omega_0 \\ \beta\widetilde{\omega}_0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & -c\omega_0 \\ -\beta\widetilde{\omega}_0\alpha & 0 \end{pmatrix} = -c \begin{pmatrix} 0 & \omega_0 \\ p\widetilde{\omega}_0 & 0 \end{pmatrix}.$$

The last matrix is the product of the first two upto a scalar factor. Hence it suffices to require M_1 to commute with the two matrices $\left(\begin{smallmatrix} p\alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & \alpha\omega_0 \\ \beta\widetilde{\omega}_0 & 0 \end{smallmatrix}\right)$. We have now to distinguish between three cases.

93 (i) $\underline{p_k \notin \mathfrak{R}^{(k)}}$ *for some* k, *(say* $k = 1$*).* Since 1, p are linearly independent over $\mathfrak{R}$, it is clear that M_1 has, of necessity, to commute with $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ 0 & \beta \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & \alpha\omega_0 \\ \beta\widetilde{\omega}_0 & 0 \end{smallmatrix}\right)$. It follows immediately that $M_1 = \left(\begin{smallmatrix} \rho & 0 \\ 0 & \rho \end{smallmatrix}\right)$ where ρ commutes with α and β and hence with all elements of ($\widehat{\mathscr{P}}$). Thus ρ is in ($\mathscr{P}$). Since $M_k = M_1^{(k)} (1 \leq k \leq h)$, we see that the rank over $\mathbb{Q}$ of the algebra of all rational matrices M_0 commuting with all R-matrices in ($\underline{\mathscr{F}}$) in this case is $4h$ which is the same as the rank of ($\mathscr{M}$) over $\mathbb{Q}$. Thus, in this case, there exist R-matrices admitting ($\mathscr{M}$) as the exact commutator-algebra.

(ii) $\underline{p \notin (\mathfrak{R})}$ *but* $\underline{p_k = |\tau^{(k)}|(1 \le k \le h)}$ *for* $\underline{\tau \in \mathfrak{R}}$.

As in case (i), we know that M_1 has to commute with $\left(\begin{smallmatrix} p\alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & \alpha\omega_0 \\ \beta\widetilde{\omega} & 0 \end{smallmatrix}\right)$. Further, for at least one $k(1 \le k \le g)$, $p_k = \tau^{(k)}$ and for some $l(1 \le l \le g)$, $p_l = -\tau^{(l)}$. Thus, from the fact that $M_k R_k = R_k M_k$ and $M_k = M_l^{(k)}$, we see that M_l has to commute with

$$\begin{pmatrix} p\alpha & 0 \\ 0 & \beta \end{pmatrix}, \begin{pmatrix} -p\alpha & 0 \\ 0 & \beta \end{pmatrix}, \begin{pmatrix} 0 & \alpha\omega_0 \\ \beta\widetilde{\omega}_0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & \alpha(-p\alpha-\beta) \\ \beta(p\alpha+\beta) & 0 \end{pmatrix}.$$

Thus, again M_l commutes with

$$\begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & \beta \end{pmatrix}, \begin{pmatrix} 0 & \alpha\beta \\ d & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & -c \\ \beta\alpha & 0 \end{pmatrix}$$

and therefore M_l has to be of the same form as in case (i) above. We conclude as above that there exist R-matrices admitting $(\mathscr{M})$ as the exact algebra of commutators.

(iii) $\underline{p \in (\mathfrak{R})}$. In this case M_l commutes with $P = \left(\begin{smallmatrix} p\alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ and $Q = \left(\begin{smallmatrix} 0 & \alpha\omega_0 \\ \beta\widetilde{\omega}_0 & 0 \end{smallmatrix}\right)$, as before. But since $P^2 = -dE_8$, $Q^2 = cp\omega_0\widetilde{\omega}_0 E_8$, $QP = -PQ$, we see that E_8, P, Q generate an abstract quaternion algebra over $\mathfrak{R}$ and this 8-rowed representation contains its irreducible representation over $\mathfrak{R}$ exactly twice. Since M_1 commutes with P, Q it follows that the rank over $\mathfrak{R}$ of the algebra formed by the matrices M_l is 16. Thus, in this case, the rank over $\mathbb{Q}$ of the algebra of rational matrices commuting with all the R-matrices in $(\widehat{\underline{\mathscr{P}}})$ is $16h$ which is greater than $4h$, the rank of $(\mathscr{M})$ over $\mathbb{Q}$. In other words, there do not exist R-matrices in $(\widehat{\underline{\mathscr{P}}})$ with $(\mathscr{M})$ as the exact algebra of commutators, in this case. **94**

For $\gamma \in (\widehat{\mathscr{P}})$, define the "reduced norm" $N_{\mathfrak{R}}(\gamma)$ of γ over $\mathfrak{R}$ by $N_{\mathfrak{R}}(\gamma) = \gamma\widetilde{\gamma}$ (which certainly belongs to $\mathfrak{R}$) and for $T_0 = \left(\begin{smallmatrix} \alpha^{-1} & 0 \\ 0 & \beta^{-1} \end{smallmatrix}\right)$ define the "reduced norm" $N_{\mathfrak{R}}(T_0)$ of T_0 by $N_{\mathfrak{R}}(T_0) = N_{\mathfrak{R}}(\alpha^{-1}\beta^{-1})$. It is then clear that $N_{\mathfrak{R}}\left(\dfrac{\alpha}{\beta}\right)$ and $N_{\mathfrak{R}}(T_0)$ are the same upto the square of a totally positive number in $\mathfrak{R}$. We conclude thus, that in the case when $\mathscr{V} = \mathscr{P}$,

$q = 2$, there exist R-matrices with $\binom{\mathscr{P}}{2}$ as exact commutator-algebra except when

$$N_{\mathfrak{R}}(T_0) = \tau^2 \quad \text{for} \quad \tau > 0 \quad \text{in} \quad \mathfrak{R}.$$

The next case for discussion is when $\mathscr{V}$ is a cyclic algebra of type (iv) with $qs = 1$ i.e. $q = s = 1$. Then $\mathscr{V}$ is the same as its centre $\mathfrak{R}(= \mathscr{Z}(\sqrt{a}))$ which is totally complex of degree 2 over a totally real subfield $\mathscr{Z}$ of degree $\frac{h}{2}$ over $\mathbb{Q}$. Let $\gamma_1, \ldots, \gamma_h$ be a basis of $\mathfrak{R}$ over $\mathbb{Q}$ and $\Omega = (\gamma_k^{(1)})(1 \leq k, l \leq h)$. Then we have

$$\begin{aligned} \Omega T_0 \Omega^{-1} &= [\tau^{(1)}, \ldots, \tau^{(h)}] \quad \text{with} \quad \tau^{(k)} = -\overline{\tau^{(k)}}, \\ \Omega N \Omega^{-1} &= [p_1, \ldots, p_h] > 0 \\ \Omega R \Omega^{-1} &= [i_1, \ldots, i_h] \end{aligned}$$

95 and necessarily $i_k = \pm\sqrt{-1}$ in view of the fact that $R^2 = -E_h$. Thus $\tau^{(k)}$ and i_k are purely imaginary and lie in opposite half-planes.

Let R be any R-matrix in $(\underline{\mathscr{F}})$ which is the same as $(\underline{\mathfrak{R}})$ and let $(\mathfrak{Q})$ denote the algebra of rational commutators (Of course, by construction, $(\mathfrak{Q})$ contains $(\mathfrak{R})$). We know $(\mathfrak{Q})$ is semi-simple but since $(\mathfrak{Q})$ is an algebra of h-rowed rational matrices containing an irreducible representation of $\mathfrak{R}$ (of degree h over $\mathbb{Q}$), we see by considering the characteristic polynomial of a generator over $\mathbb{Q}$ of $(\mathfrak{R})$, that $(\mathfrak{Q})$ is necessarily simple. Let then $(\mathfrak{Q})$ be the total matrix-algebra of order 1 over a division algebra $\mathscr{V}_1$ and let $\mathscr{V}_1$ be a division algebra with centre $\mathfrak{g}$ which is an algebraic number field of degree g over $\mathbb{Q}$. By considering the representation of a generator of $\mathfrak{R}$ over $\mathbb{Q}$ with respect to a splitting field of $\mathscr{V}_1$, we see that $\mathscr{V}_1 = \mathfrak{g}$. Now the degree of a maximal commutative system in $(\mathfrak{Q})$ is necessarily gl and it is easy to deduce that $gl = h$ and $(\mathfrak{g}) \subset (\mathfrak{R})$. Let $\mathfrak{g}^{(1)}(= \mathfrak{g}), \mathfrak{g}^{(2)}, \ldots, \mathfrak{g}^{(g)}$ be the conjugates of $\mathfrak{g}$ over $\mathbb{Q}$. Let $\mathfrak{R}^{(1)}(= \mathfrak{R})$, $\mathfrak{R}^{(2)}, \ldots, \mathfrak{R}^{(1)}$ be the conjugates of $\mathfrak{R}$ over $\mathfrak{g}^{(1)}$ and $\mathfrak{R}^{(1+1)}, \ldots, \mathfrak{R}^{(21)}$ the conjugates of $\mathfrak{R}^{(1+1)}$ over $\mathfrak{g}^{(2)}$ and so on. Taking a representation over $\mathfrak{g}^{(1)}, \ldots, \mathfrak{g}^{(g)}$, let $T_0 = [T^{(1)}, \ldots, T^{(g)}]$ and $R = [R_1, \ldots, R_g]$. Since $\mathscr{M}_1((\mathfrak{g}))$ is the complete rational commutator-algebra of R, it follows
96 that $R_k = \pm iE_l$ (for $1 \leq k \leq g$). Thus $i\tau^{(kl+1)}, \ldots i\tau^{(kl+1)}$ have all the same sign (for $1 \leq k \leq g$). If $\mathfrak{Q} = (\mathfrak{R})$, then we must have necessarily $l = 1$

and $g = h$. The criterion for R to have $(\mathfrak{R})$ an exact commutator-algebra is then clearly that l should not be greater than 1. We may reformulate this condition as follows, namely, that there should exist no proper subfield $\mathfrak{g}$ of $\mathfrak{R}$ such that the conjugates of τ with respect to each conjugate $\mathfrak{g}^{(k)}$ of $\mathfrak{g}$ should not all lie in the same complex half-plane (lower or upper). In other words, $\sqrt{a}T_0$ *should not be totally-definite over any proper subfield* $\mathfrak{g}$ *of* $\mathfrak{R}$.

We proceed to discuss the case when $\mathscr{V} = \mathfrak{R}$ of type (iv) but $q = 2$. Then $\mathfrak{R} = \mathscr{Z}(\sqrt{a})$ with $\mathscr{Z}$ totally real and $-a > 0$ in $\mathscr{Z}$. For $\alpha = x + y\sqrt{a}$ in $\mathfrak{R}$ with $x, y \in \mathscr{Z}$, we always take the 2-rowed representation $\left(\begin{smallmatrix} x & y \\ ay & x \end{smallmatrix}\right)$ over $\mathscr{Z}$ and denote it by α again. For $\alpha = \left(\begin{smallmatrix} x & y \\ ay & x \end{smallmatrix}\right) \in \mathfrak{R}$, $\widetilde{\alpha} = \overline{\alpha} = \left(\begin{smallmatrix} x & -y \\ -ay & x \end{smallmatrix}\right)$. In particular, to $\sqrt{a}$ corresponds $\varepsilon = \left(\begin{smallmatrix} 0 & 1 \\ a & 0 \end{smallmatrix}\right)$. Any $\alpha = x + y\sqrt{a} \in \mathfrak{R}$, is then equal to $xE_2 + y\varepsilon$. If $\mathscr{Z}^{(k)}$ is a conjugate of $\mathscr{Z}$ over $\mathbb{Q}$, then corresponding to $\alpha = \left(\begin{smallmatrix} x & y \\ ay & x \end{smallmatrix}\right)$ in $\mathfrak{R}$, we define $\alpha^{(k)}$ by $\left(\begin{smallmatrix} x^{(k)} & y^{(k)} \\ (ay)^{(k)} & x^{(k)} \end{smallmatrix}\right)$. Let $\gamma_1, \ldots, \gamma_g$ be a basis of $\mathscr{Z}$ over $\mathbb{Q}$ and $\Omega = (\gamma_k^{(1)})(1 \leq k, l \leq g)$. For elements T of $\mathscr{F}$, we have first a representation $T = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ over $\mathscr{Z}$, where $\alpha, \beta, \gamma, \delta$ are in $\mathfrak{R}$ and a rational representation for T is given by

$$(\Omega \times E_4)[T^{(1)}, \ldots, T^{(g)}](\Omega \times E_4)^{-1} \text{ where } T^{(k)} = \begin{pmatrix} \alpha^{(k)} & \beta^{(k)} \\ \gamma^{(k)} & \delta^{(k)} \end{pmatrix}.$$

We shall in the sequel, use sometimes for the elements T of $\mathscr{F}$, the representation $(\mathscr{F})$ given by $T \to [T^{(1)}, \ldots, T^{(g)}]$ over $\mathscr{Z}$ and its con- **97**
jugates as mentioned above. We then extend this representation linearly to the linear closure $(\underline{\mathscr{F}})$ of $(\mathscr{F})$. When there is no risk of confusion, we shall denote $T \in (\mathscr{F})$ merely by $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ as above without referring to all the g components every time.

Let then $T_0 = -\widetilde{T}_0$ be a nonsingular element of $(\mathscr{F})$. By the same arguments as in the case $\mathscr{V} = \mathscr{P}$, $q = 2$, we can suppose that $T_0^{-1} = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ with $\alpha = -\widetilde{\alpha}$, $\beta = -\widetilde{\beta}$ in $\mathfrak{R}$. Let $N = [N_1, \ldots, N_g]$ with $N_k = \left(\begin{smallmatrix} x_k & z_k \\ \overline{z}_k & y_k \end{smallmatrix}\right)$ be in $(\underline{\mathscr{F}})$, satisfying $N = \widetilde{N}$ and having all eigenvalues real and positive. It follows that x_k, y_k are positive real scalar multiples of E_2, while $Z_k = c_k E_2 + d_k \varepsilon$ with $c_k, d_k \in \mathbb{R}$ and further $x_k y_k - z_k \overline{z}_k > 0$.

Let now $R = T_0^{-1}N$ be an R-matrix in ($\underline{\mathscr{F}}$). Then

$$R = (\Omega \times E_4)[R_1, \ldots, R_g](\Omega \times E_4)^{-1} \tag{92}$$

with $R_k = \left(\begin{smallmatrix} \xi_k & \eta_k \\ \zeta_k & \tau_k \end{smallmatrix}\right)$ and $\xi_k = x_k\alpha^{(k)}$, $\eta_k = \alpha^{(k)}z_k$, $\zeta_k = \beta^{(k)}\overline{z}_k$, $\tau_k = y_k\beta^{(k)}$. Now $R_2 = -E$ gives, for $1 \leq k \leq g$,

$$\xi_k^2 + \eta_k\zeta_k = -1, \tau_k^2 + \eta_k\zeta_k = -1, (\xi_k + \tau_k)\eta_k = 0 = (\xi_k + \tau_k)\zeta_k \tag{93}$$

Now there are two possibilities, namely, either a) $\xi_k + \tau_k \neq 0$, in which case we have necessarily $\zeta_k = 0 = \eta_k$, or b) $\xi_k + \tau_k = 0$. In case a),
98 we see that $R_k = \left(\begin{smallmatrix} \xi_k & 0 \\ 0 & \tau_k \end{smallmatrix}\right)$, where, from (93), $\xi_k = \pm\dfrac{1}{\sqrt{-a^{(k)}}}\varepsilon^{(k)}$, $\tau_k = \pm\dfrac{1}{\sqrt{-a^{(k)}}}\varepsilon^{(k)}$. Since $\xi_k + \tau_k \neq 0$, it follows that $\xi_k = \tau_k = \pm\dfrac{1}{\sqrt{-a^{(k)}}}\varepsilon^{(k)}$ and thus

$$R_k = \pm\frac{1}{\sqrt{-a^{(k)}}}\begin{pmatrix} \epsilon^{(k)} & 0 \\ 0 & \epsilon^{(k)} \end{pmatrix} \tag{94}$$

Now $\xi_k = \tau_k$ is equivalent to the fact that $\dfrac{\alpha^{(k)}}{\beta^{(k)}} = \dfrac{y_k}{x_k} > 0$, which, in turn, is equivalent to the fact that $a_kb_k = 0$, in our former notation. Let us now consider case b), when $\xi_k + \tau_k = 0$ or equivalently $\dfrac{\alpha^{(k)}}{\beta^{(k)}} = -\dfrac{y_k}{x_k} < 0$. Thus, in this case, $a_kb_k = 1$. Now $\xi_k = -\tau_k$ and we have

$$R_k = \begin{pmatrix} x_k\alpha^{(k)} & \alpha^{(k)} \\ \beta^{(k)}\overline{z}_k & -x_k\alpha^{(k)} \end{pmatrix} \tag{95}$$

From (93), we obtain $(x_k\alpha^{(k)})^2 + \alpha^{(k)}\beta^{(k)}x_k\overline{z}_k = -1$, i.e.

$$-(\alpha^{(k)})^2x_k^2 - \alpha^{(k)}\beta^{(k)}z_k\overline{z}_k = 1 \tag{96}$$

Since $\overline{\alpha^{(k)}} = -\alpha^{(k)}$, $\overline{\beta^{(k)}} = -\beta^{(k)}$, it is clear that $-(\alpha^{(k)})^2 > 0$ while $-\alpha^{(k)}\beta^{(k)} < 0$. Thus equation (96) defines a two-sheeted hyperboloid in the x_k, z_k-space. As a consequence of (96), we also have $-\dfrac{\alpha^{(k)}}{\beta^{(k)}}x_k^2 - z_k\overline{z}_k = \dfrac{1}{\alpha^{(k)}\beta^{(k)}} > 0$ which means $x_ky_k - z_k\overline{z}_k > 0$.

We may rule out the possibility that when case a) could occur for all the g components, since then $a_k b_k = 0$ for all k and this case has been discussed already.

So then let us assume that at least one component of R, say R_1, without loss of generality is of the form (95). Let M be a rational matrix **99** commuting with all R-matrices in ($\underline{\mathscr{F}}$). Then using the form (92) for R-matrices, $M_1 = (\Omega \times E_4)^{-1} M (\Omega \times E_4)$ commutes with $[R_1, \ldots, R_g]$. We split up M_1 as $(M_{kl})(1 \leq k, l \leq g)$ with 4-rowed square matrices M_{kl}. Now in R_1, the three real parameters in x_1, z_1 are linearly independent and therefore $M_{21} = 0 = \ldots = M_{gl}$. We are now in a position to apply Lemma 3 and deduce that all the elements of M_{11} are in $\mathscr{Z}$ while $M_{kk} = M_{11}^{(k)}$ and $M_{kl} = 0$ for $k \neq 1$. Further $M_{kk} R_k = R_k M_{kk}$.

Let us now suppose that *not all of the components R_k are of the form* (95) *i.e. neither $a_k b_k = 0$ for all k nor $a_k b_k = 1$ for all k.* Further, without loss of generality, let R_1 be of the form (95) while R_2 is of the form (94). Then writing $M_{22} = \left(\begin{smallmatrix} \lambda & \mu \\ \kappa & \nu \end{smallmatrix}\right)$ with 2-rowed square matrices λ, κ, μ, ν having elements in $\mathscr{Z}^{(2)}$, we obtain each one of them commutes with $\varepsilon^{(2)} = \left(\begin{smallmatrix} 0 & 1 \\ a^{(2)} & 0 \end{smallmatrix}\right)$ and therefore λ, κ, μ, ν represent elements in $\mathscr{Z}^{(2)}(\sqrt{a^{(2)}})$. Since $M_{kk} = M_{11}^{(k)}$, we know M_{11}, $M_{22}, \ldots, M_{gg}$ are conjugate over $\mathscr{Z}$ and hence the elements of M_{kk} are in $\mathscr{Z}^{(k)}(\sqrt{a}^{(k)})$ and in particular M_{11} has elements in $\mathfrak{R}$.

From $M_{11} R_1 = R_1 M_{11}$ for all R_1 of the form (95) it follows that M_{11} has to commute with $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & -\alpha \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & \alpha \\ \beta & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & \alpha\varepsilon \\ -\beta\varepsilon & 0 \end{smallmatrix}\right)$ (dropping the suffixes and superscripts). Let us now set $\beta\alpha^{-1} = p$; p lies in $\mathscr{Z}$, in fact. The matrix M_{11} which already commutes with $\left(\begin{smallmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{smallmatrix}\right)$ has also to commute with

$$A = \begin{pmatrix} \varepsilon & 0 \\ 0 & -\varepsilon \end{pmatrix}, B = \begin{pmatrix} 0 & \varepsilon \\ -p\varepsilon & 0 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} 0 & \varepsilon^2 \\ +p\varepsilon^2 & 0 \end{pmatrix} = AB = -BA \tag{97}$$

Thus M_{11} has to commute with $\left(\begin{smallmatrix} \varepsilon & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ 0 & \varepsilon \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & \varepsilon \\ -p\varepsilon & 0 \end{smallmatrix}\right)$. Therefore **100** $M_{11} = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ with $\lambda \in \mathfrak{R}$. Hence the rank over $\mathbb{Q}$ of the algebra of rational matrices commuting with all R-matrices in ($\underline{\mathscr{F}}$) is $2 \cdot g = h$ which is exactly the rank of $\mathscr{M}$ over $\mathbb{Q}$. We conclude, as before, that in this case, there exist R-matrices with ($\mathscr{M}$) as exact commutator-algebra.

On the other hand, let all R_k be of the form (95). The M_{11} is an arbitrary 4-rowed square matrix with elements in $\mathscr{Z}$ and commuting with A, B and C as defined in (97). But from (97) and from $A^2 = aE$, $B^2 = -paE$, we see that 1, A, B generate a quaternion algebra Φ over $\mathscr{Z}$ and M_{11} has then to lie precisely in the commutator-algebra of Φ. Hence the rank of the algebra of all rational matrices commuting with all the R-matrices in ($\underline{\mathscr{F}}$) is precisely $4g = 2h$ which is greater than the rank of $\mathscr{M}$ over $\mathbb{Q}$. Thus in the case when $a_k b_k = 1$ for all k, there exist no R-matrix with ($\mathscr{M}$) as its exact commutator-algebra. Now $a_k b_k = 1$ for all k or $a_k b_k = 0$ for all k is respectively equivalent to the fact that εT_0 is totally indefinite or totally definite over $\mathfrak{R}$. Or, putting it in other words, except when $|T_0|^{-1} = \alpha\beta$ (by definition) is either totally positive or totally negative in $\mathscr{Z}$, there exist R-matrices with ($\mathscr{M}$) as the exact algebra of commutators.

We now deal with the last of the exceptional cases, namely when $\mathscr{V}$ is a cyclic algebra of type (iv) and $s = 2$, $q = 1$. Thus $\mathscr{V}$ is a quaternion algebra with centre $\mathfrak{R}$ which is obtained by adjoining $\epsilon = \sqrt{a}$ to a totally
101 real field $\mathscr{Z}$ of degree g over $\mathbb{Q}$ and $-a > 0$ is in $\mathscr{Z}$. As before, we can find a totally real field $\mathfrak{Z}_0 = \mathfrak{Z}(\rho)$ with $\rho = \sqrt{d}$ and $d > 0$ in $\mathscr{Z}$ such that $\mathfrak{Z} = \mathfrak{Z}_0(\varepsilon)$ serves as a splitting field for $\mathscr{V}$. There are two automorphisms in $\mathfrak{g}$ which are identity on $\mathscr{Z}$ and commute with each other, namely for $\xi \in \mathfrak{Z}$,

$$\xi = x + y\rho \to \dot{\xi} = x - y\rho (x, y \in \mathfrak{R})$$
$$\xi = p + q\varepsilon \to \overline{\xi} = p - q\epsilon (p, q \in \mathfrak{Z}_0)$$

The algebra $\mathscr{V}$ is generated over $\mathfrak{Z}$ by an element $\mathfrak{J}$ which satisfies $\mathfrak{J}^2 = b \in \mathfrak{R}$ and $\mathfrak{J}\xi = \dot{\xi}\mathfrak{J}$. Further, there exists $c \in \mathfrak{Z}_0$ such that $c\dot{c} = b\overline{b}$. For $\eta \in \mathfrak{Z}_0$, the mapping $\eta \to \dot{\eta}$ is an automorphism of $\mathfrak{Z}_0$ over $\mathscr{Z}$.

For $\delta = \xi + \eta j \in \mathscr{V}$ with $\xi, \eta \in \mathfrak{Z}$, we have over $\mathfrak{Z}$ the representation $\delta \to D = \begin{pmatrix} \xi & \eta \\ \dot{b}\dot{\eta} & \dot{\xi} \end{pmatrix}$. Further $\dot{D} = \begin{pmatrix} \dot{\xi} & \dot{\eta} \\ b\dot{\eta} & \dot{\xi} \end{pmatrix} = \mathscr{F} D \mathscr{F}^{-1}$ where $\mathscr{F} = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$. In terms of D, the positive involution in $\mathscr{V}$ is expressed as

$$\begin{pmatrix} \xi & \eta \\ \dot{b}\dot{\eta} & \dot{\xi} \end{pmatrix} = D \to \widetilde{D} = F^{-1}\overline{D}'F = \begin{pmatrix} \overline{\xi} & \dot{c}\dot{\overline{\eta}} \\ \dot{b}\dot{\overline{\eta}} & \dot{\overline{\xi}} \end{pmatrix}, F^{-1} = [c, c\dot{c}] > 0 \qquad (98)$$

We obtain for $\mathscr{V}$, a representation $\delta \to D_0 = (\Omega_1 \times E_2)[D\overline{D}](\Omega_1 \times E_2)^{-1}$ where $\Omega_1 = \begin{pmatrix} 1 & 1 \\ \varepsilon & -\varepsilon \end{pmatrix}$. It is clear that $D_0 = \begin{pmatrix} \xi & \eta \\ \mathfrak{b}\dot{\eta} & \dot{\xi} \end{pmatrix}$ where now ξ, η, $b\dot{\eta}$, $\dot{\xi}$ stand for their 2-rowed representations over $\mathfrak{Z}_0$ with respect to the basis 1, ε. From this, we pass to a representation of $\mathscr{V}$ over $\mathscr{Z}$ given by $\delta \to \underline{D} = K_1[D_0\dot{D}_0]K_1^{-1}$ where $K_1 = \Omega_2 \times E_4$, $\Omega_2 = \begin{pmatrix} 1 & 1 \\ \rho & -\rho \end{pmatrix}$ and then to the rational representation

$$\delta \to (\Omega_3 \times E_8)[\underline{D}^{(1)}, \ldots, \underline{D}^{(g)}](\Omega_3 \times E_8)^{-1} \tag{99}$$

where $\Omega_3 = (\gamma_k^{(1)})$, $\gamma_1, \ldots, \gamma_g$ being a basis of $\mathscr{Z}$ over $\mathbb{Q}$. **102**

For the abstract algebra, we may start with the regular representation of its opposite algebra and assume that for the elements of the commutator algebra $(\mathscr{F})$ of $(\mathscr{V})$, we already have the rational representation of the form (99). (Let us remark that this arrangement is purely for the sake of convenience in working. Even if we had started with the regular representation $(\mathscr{V})$ of the abstract algebra $\mathscr{V}$, the positive involution in $(\mathscr{V})$ will correspond to the involution $T \to \widetilde{T} = \dot{F}^{-1}\overline{T}'\dot{F}$ in $(\mathscr{F})$. This is different from (98) only in as much as F has to be replaced by $\dot{F}$ but observe that this involution is again positive).

Let $T_0 = -\widetilde{T}_0$ be a nonsingular element of $(\mathscr{F})$ and let $T_0 = (\Omega_3 \times E_8)[\underline{T}_0^{(1)}, \ldots, \underline{T}_0^{(g)}](\Omega_3 \times E_8)^{-1}$ where $\underline{T}_0^{(k)}$ are defined as follows. Let T_0 have the representation $\begin{pmatrix} \alpha & \beta \\ \mathfrak{b}\beta & \dot{\alpha} \end{pmatrix}$ over $\mathfrak{Z}$ and let $\mathfrak{Z}^{(k)} = \mathscr{Z}^{(k)}(\sqrt{d^{(k)}}, \sqrt{a^{(k)}})$. Define $\alpha^{(k)}, \beta^{(k)}, (b\dot{\beta})^{(k)}, (\dot{\alpha})^{(k)}$ to be the images of $\alpha, \beta, b\dot{\beta}, \dot{\alpha}$ respectively under the isomorphism of $\mathfrak{Z}$ onto $\mathfrak{Z}^{(k)}$ taking $\mathscr{Z}$ onto $\mathscr{Z}^{(k)}$. Then

$$\underline{T}_0^{(k)} = \begin{pmatrix} \alpha^{(k)} & \beta^{(k)} \\ (b\dot{\beta})^{(k)} & (\dot{\alpha})^{(k)} \end{pmatrix} \tag{100}$$

where for the elements of $\underline{T}_0^{(k)}$, we have taken their regular representation over $\mathscr{Z}^{(k)}$. From $\widetilde{T}_0 = -T_0$, we obtain $\alpha = -\overline{\alpha}, \beta = -\frac{c}{b}\overline{\beta}, b\dot{\beta} = -\dot{c}\overline{\beta}$, $\dot{\alpha} = -\dot{\overline{\alpha}}$ or $\overline{\alpha} - \alpha, b\dot{\beta} = -\dot{c}\overline{\beta}$. Let $N = (\Omega_3 \times E_8)[N_1, \ldots, N_g](\Omega_3 \times E_8)^{-1}$ be in $(\mathscr{F})$ having the properties mentioned in (86) and analogous to

(100), let $N_k = \begin{pmatrix} \lambda_k & \mu_k \\ b^{(k)}\dot{\mu}_k & \dot{\lambda}_k \end{pmatrix}$ where λ_k, μ_k are in the linear closure of **103**
$\mathfrak{Z}^{(k)}$ and hence commute with elements of $\mathfrak{Z}^{(k)}$. Then $\lambda_k = \overline{\lambda}_k$ and $b\dot{\mu} = \dot{c}\overline{\mu}$. Further N_k has all its eigenvalues real and positive i.e. $\lambda_k\dot{\lambda}_k - b^{(k)}\mu_k\dot{\mu}_k > 0$. Now $R = T_0^{-1}N$ is a R-matrix in ($\underline{\mathscr{F}}$) and let again $R = (\Omega_3 \times E_8)[R_1, \ldots, R_g](\Omega_3 \times E_8)^{-1}$ with $R_k = \begin{pmatrix} \overline{\xi}_k & \eta_k \\ b^{(k)}\dot{\eta}_k & \dot{\xi}_k \end{pmatrix}$. From $R^2 = -E$, we obtain,

$$\xi_k^2 + b^{(k)}\eta_k\dot{\eta}_k = -1 = \dot{\xi}_k^2 + b^{(k)}\eta_k\dot{\eta}_k, \quad (\xi_k + \dot{\xi}_k)\eta_k = 0 = (\xi_k + \dot{\xi}_k)b^{(k)}\dot{\eta}_k \tag{101}$$

Let us denote $\alpha\dot{\alpha} - b\beta\dot{\beta}$ by δ. Then $\delta \in \mathscr{Z}$. We know that $\delta^{(k)}$ is negative or positive according as $a_kb_k = 0$ or 1 respectively, in our former notation. On the other hand, taking determinants, $|R_k|\delta^{(k)} = |N_k|$ which, in view of (86) is positive. Further, since $R^2 = -E$, we have $|R_k| = \pm 1$. Now, in (101), one of two possibilities arises, namely, either a) $\xi_k + \dot{\xi}_k \neq 0$, in which case $\eta_k = 0$, $\dot{\eta}_k = 0$, or b) $\xi_k = -\dot{\xi}_k$.

In case a), using (101), we see that $\xi_k = \dot{\xi}_k = \pm\dfrac{1}{\sqrt{a^{(k)}}}\varepsilon^{(k)}$. Since we $|R_k| = -1$, we see that $\delta^{(k)} < 0$ and thus case a) corresponds to the situation when $a_kb_k = 0$ and then

$$R_k = \pm\frac{1}{\sqrt{a^{(k)}}}\begin{pmatrix} \varepsilon^{(k)} & 0 \\ 0 & \varepsilon^{(k)} \end{pmatrix} \tag{102}$$

When case b) occurs, $\xi_k = -\dot{\xi}_k$ and therefore $|R_k| = -\xi_k^2 - b^{(k)}\eta_k\dot{\eta}_k = 1$, in view of (101). Thus case b) corresponds precisely to the situation
104 $\delta^{(k)} > 0$ or equivalently $a_kb_k = 1$. Thus in case b), $R_k = \begin{pmatrix} \xi_k & \eta_k \\ b^{(k)}\dot{\eta}_k & -\xi_k \end{pmatrix}$ and R_k contains "a priori" eight free real parameters. From $N_k = \underline{T}_0^{(k)}R_k$, we obtain, dropping the inconvenient suffix k and the superscript k everywhere without risk of confusion, that

$$\lambda = \alpha\xi + b\beta\dot{\eta}, \mu = \alpha\eta - \beta\xi, \dot{\lambda} = b\dot{\beta}\eta - \dot{\alpha}\xi, b\dot{\mu} = b(\dot{\beta}\xi + \dot{\alpha}\dot{\eta}) \tag{103}$$

Since $\alpha = -\overline{\alpha}$, $\varepsilon = -\overline{\varepsilon}$, $\lambda = \overline{\lambda}$ and $\alpha\beta \neq 0$, we can define $r = \overline{r}$, $s = \overline{s}$ by

$\lambda = \alpha\varepsilon r$, $\dot{\lambda} = \dot{\alpha}\varepsilon s$. Then from (103), we have

$$b\dot{\beta}\eta = \dot{\alpha}(\xi + \varepsilon s), b\beta\dot{\eta} = \alpha(\varepsilon\gamma - \xi) \tag{104}$$

But, from $N = \tilde{N}$, we have $b\dot{\mu} = \dot{c}\overline{\mu}$ and again, in view of (103),

$$\dot{c}(-\alpha\overline{\eta} - \overline{\beta\xi}) = b(\dot{\beta}\xi + \dot{\alpha}\dot{\eta}) \tag{105}$$

Multiplying both sides of (105) by β and using (103), (104), we obtain

$$\begin{aligned} b\beta\dot{\beta}\xi + \alpha\dot{\alpha}(\varepsilon r - \xi) &= -\dot{c}\beta\overline{\eta}\alpha - \dot{c}\beta\overline{\beta\xi} \\ &= \overline{b}\overline{\dot{\beta}}\overline{\eta}\alpha + b\beta\dot{\beta}\overline{\xi} \\ &= -\alpha\dot{\alpha}(\overline{\varepsilon s + \xi}) + b\beta\dot{\beta}\overline{\xi} \\ &= \alpha\dot{\alpha}(\varepsilon s - \overline{\xi}) + b\beta\dot{\beta}\overline{\xi} \end{aligned}$$

Thus

$$\frac{1}{2}(\xi - \overline{\xi}) = \frac{\alpha\dot{\alpha}}{\delta}\varepsilon \cdot \frac{1}{2}(r - s) \tag{106}$$

While r, s and $t = \frac{1}{2}(\xi + \overline{\xi})$ are free, the imaginary part of ξ is fixed by (106). We now set

$$u = b\frac{\beta\dot{\beta}}{\delta}\frac{r - s}{2}, \quad v = \frac{r + s}{2}, q = \frac{\alpha\dot{\alpha}}{b\beta\dot{\beta}}$$

Then obviously $q \in \mathscr{Z}$ and furthermore, since $b\beta\dot{\beta} = -\dot{c}\beta\overline{\beta} < 0$ and $\delta > 0$, we have

$$q - 1 < 0 \tag{107}$$

From (106), we have $\xi = t + q\varepsilon u$. From (104), we get

$$\frac{b\dot{\beta}}{\dot{\alpha}}\eta = \varepsilon s + \xi = t + \varepsilon(u + v) \tag{108}$$

and similarly **105**

$$\frac{b\beta}{\alpha}\dot{\eta} = \varepsilon r - \xi = -t + \varepsilon(v - u) \tag{109}$$

Thus t, u, v are real parameters which, in view of (108) and (109) are subject to the conditions

$$\dot{t} = -t, \quad \dot{u} = -u, \quad \dot{v} = v \tag{110}$$

The relation $\xi^2 + b\eta\dot{\eta} = -1$ can be rewritten in terms of u, v, t as $\xi^2 + \frac{\alpha\dot{\alpha}}{b\beta\dot{\beta}} \cdot \frac{b\dot{\beta}\eta}{\alpha} \cdot \frac{b\beta\dot{\eta}}{\dot{\alpha}} = -1$ and using (108) and (109), we obtain

$$(t + q\varepsilon u)^2 + q(t + \varepsilon(v + u))(-t + \varepsilon(v - u)) = -1$$

i.e.

$$(1 - q)t^2 - aq(1 - q)u^2 + aqv^2 = -1 \tag{111}$$

In view of (107), exactly one of aq and $-aq(1 - q)$ is a negative while the coefficient of t^2 is positive. Further for t, u, v satisfying (111), $r \neq 0$. For, if $r = 0$, we should necessarily have $(1-q)t^2 - aq(1-q)\left(\frac{b\beta\dot{\beta}}{2\delta}\right)^2 s^2 + aq\frac{s^2}{4} = -1$. But the left hand side is just $(1 - q)t^2 - \frac{aq^2}{4(1-q)}s^2$ which is always non-negative. We thus see that in the t, u, v-space, equation (111) defines a "two-sheeted hyperboloid".

Thus in the case when $a_k b_k = 1$, using (108) and (109), we have for R_k the parametrization

$$R_k = V_k \begin{pmatrix} t^k + qu_k\varepsilon^{(k)} & q(t_k + \varepsilon^{(k)}(u_k + v_k)) \\ -t_k + \varepsilon^{(k)}(-u_k + v_k) & -t_k - qu_k\varepsilon^{(k)} \end{pmatrix} V_k^{-1} \tag{112}$$

106 where $V_k = [1, (\frac{\alpha}{\beta})^{(k)}]$.

We proceed to discuss the algebra of commutators of the R-matrices R. As before, we rule out the occurrence of case a) for all the g components of R. Let then at least one component of R, say R_1, be of the form (112). If M is a rational matrix commuting with all R-matrices in

($\underline{\mathscr{F}}$), then $M_1 = (\Omega_3 \times E_8)^{-1} M (\Omega_3 \times E_8)$ commutes with $[R_1, \ldots, R_g]$ and by the same arguments as on p.99, $M_1 = [M_{11}^{(1)}, \ldots, M_{11}^{(g)}]$ where $M_{11} = M_{11}^{(1)}$ is an 8-rowed square matrix with elements in $\mathscr{Z}$ commuting with

$$R_1 = \left[V_1 \begin{pmatrix} t_1 + q\varepsilon u_1 & q(t_1 + \varepsilon(v_1 + u_1)) \\ -t_1 + \varepsilon(v_1 - u_1) & -t_1 - q\varepsilon u_1 \end{pmatrix} V_1^{-1}, \right.$$
$$\left. \dot{V}_1 \begin{pmatrix} -t_1 - q\varepsilon u_1 & q(-t_1 + \varepsilon(v_1 - u_1)) \\ t_1 + \varepsilon(v_1 + u_1) & t_1 + q\varepsilon u_1 \end{pmatrix} \dot{V}_1^{-1} \right] \qquad (113)$$

For the elements of the matrices in (113) of which R_1 is a direct sum, we have taken the Z-rowed representation over the linear closure of $\mathfrak{Z}_0$ so that R_1 is an 8-rowed square matrix. Taking into account the relations $\dot{t}_1 = -t_1$, $\dot{u}_1 = -u_1$ and $\dot{v}_1 = v_1$ and replacing t_1 by $\sqrt{d}t_1$, u_1 by $\sqrt{d}u_1$, we see that M_{11} has to commute with $[V_1, \dot{V}_1]A[V_1, \dot{V}_1]^{-1}$, $[V_1, \dot{V}_1]B[V_1, \dot{V}_1]^{-1}$ and $[V_1, \dot{V}_1]C[V_1, \dot{V}_1]^{-1}$ where

$$A = \left[\sqrt{d} \begin{pmatrix} 1 & q \\ -1 & -1 \end{pmatrix}, -\sqrt{d} \begin{pmatrix} 1 & q \\ -1 & -1 \end{pmatrix} \right],$$
$$B = \left[\sqrt{d}\varepsilon \begin{pmatrix} q & q \\ -1 & -q \end{pmatrix}, -\sqrt{d}\varepsilon \begin{pmatrix} q & q \\ -1 & -q \end{pmatrix} \right]$$
$$C = \left[\varepsilon \begin{pmatrix} 0 & q \\ 1 & 0 \end{pmatrix}, \varepsilon \begin{pmatrix} 0 & q \\ 1 & 0 \end{pmatrix} \right] \qquad (114)$$

For the elements in the matrices in (114). We have taken the 2-rowed representation over $\mathfrak{Z}_0$. **107**

Let us now suppose at least one of the components of R is of the form (102). Then we can conclude as on p.99, M_{11} has elements in $\mathfrak{R}$. But now it is easy to verify that the matrices A, B, C defined by (114) satisfy

$$A^2 = d(1-q)E, \quad C^2 = aqE, \quad AC = B = -CA$$

and therefore generate a quaternion algebra Φ over $\mathfrak{R}$. The matrices M_{11} belong to the commutator algebra of Φ over $\mathfrak{R}$ and therefore constitute an algebra of rank 8 over $\mathscr{Z}$. We may then conclude that the algebra of

all the rational matrices commuting with all the R-matrices in ($\underline{\mathscr{F}}$) is, in this case, exactly $8g = 4h$ which is nothing but the rank of ($\mathscr{M}$) over $\mathbb{Q}$.

Finally, let us suppose that all the components of R are of the form (112) i.e. $a_k b_k = 1$ for all k. Then M_{11} is, as before, an 8-rowed square matrix with elements in $\mathscr{Z}$ which commutes with the 8-rowed representation of Φ over $\mathscr{Z}$. But this latter representation of Φ contains the irreducible representation of Φ over $\mathscr{Z}$ exactly twice and therefore, it is clear that the matrices M_{11} generate an algebra of rank 16 over $\mathscr{Z}$. It is now immediate that the algebra of all rational matrices M commuting with all the R-matrices in ($\underline{\mathscr{F}}$) is, in this case, equal to $16g = 8h$ which is greater than the rank of ($\mathscr{M}$) over $\mathbb{Q}$.

108 Thus, in the case when $\mathscr{V}$ is of type (iv) and $s = 2$, $q = 1$, there exist R-matrices with ($\mathscr{M}$) as exact commutator-algebra unless εT_0 is totally - definite hermitian or totally indefinite hermitian over $\mathfrak{R}$.

We shall say T_0 is *skew-symmetric totally definite* or *totally indefinite* according as εT_0 is totally definite hermitian or totally indefinite hermitian.

We have thus completely solved our problem on Riemann matrices and we may summarize our results in the following theorem. (We remark that the matrix T_0, which appears in the statement of Theorem 7, is precisely the given non-singular matrix in ($\mathscr{F}$) which is skew-symmetric for the involution in ($\mathscr{F}$) and $A = \underset{q}{G} T_0$ is a principal matrix for our R-matrices).

Theorem 7. *With the notation of Theorem 5, there always exists a R-matrix with the given A as principal matrix and having* ($\mathscr{M}$) = ($\mathfrak{g}$) *as the exact algebra of commutators except when*

a) $\mathscr{V} = \mathfrak{R}$ *with a positive involution of the first kind, q is odd*

b) $\mathscr{V} = \mathscr{P}$, $q = 1$.

c) $\mathscr{V} = \mathscr{P}$, $q = 2$, $N_{\mathfrak{R}}(|T_0|) = \tau^2$ *for* $\tau > 0$ *in* $\mathfrak{R}$.

d) $\mathscr{V}$ *is of type* (iv), $q = s = 1$ *and there exists a proper subfield* $\mathfrak{J}$ *of* $\mathscr{V} = \mathfrak{R}$ *over which iT_0 is totally definite.*

e) *$\mathscr{V}$ is of type* (iv), *$s = 1$, $q = 2$ and T_0 is skew-symmetric totally definite or totally indefinite over $\mathscr{V} = \mathfrak{R}$, and*

f) *$\mathscr{V}$ is of type* (iv), *$s = 2$, $q = 1$ and T_0 is skew-symmetric totally definite or totally indefinite over the centre $\mathfrak{R}$.*

Remarks. (1) In solving our problem on *R*-matrices, we have allowed for *A* the fullest possible generality; we emphasize that the transformations which we performed on $(\overline{\mathscr{F}})$ there, to reduce *A* to the simple form J, were merely to make the discussion easier and constituted no diminution of the generality of *A*. **109**

(2) Suppose $\mathscr{V}$ is of type (iv), $\mathscr{Z} = \mathbb{Q}$ and $qs = 2$. Then *there cannot exist nonsingular* $T_0 = -\widetilde{T}_0$ in $(\mathscr{F})$ which are neither skew-symmetric totally definite nor skew-symmetric totally indefinite over $\mathfrak{R}$ (which is now an imaginary quadratic extension of $\mathbb{Q}$), since there cannot exist in $\mathbb{Q}$ non-zero numbers which are neither positive nor negative!

8 Modular groups associated with Riemann matrices

In this concluding section, we shall make a close study of the space $\mathscr{F}$ which we associated on p. 56 with the given division algebra $\mathscr{V}$. We shall see, for example, how far $(\mathscr{M}) = (\underset{q}{\mathscr{V}})$ determines $\mathscr{M}$ and find all the principal matrices for a general *R*-matrix. Later we shall define the general modular groups which act on $\mathscr{F}$ as groups of transformations of $\mathfrak{H}$ onto itself. The scope of these lectures prevents us from making a function-theoretic study of these modular groups analogous to some recent work of I. I. Pyatetskii Shapiro ([13], [14]). We merely remark that the preparatory material for this study is contained in [21] and [22].

We may first briefly recall how $\mathfrak{H}$ was defined. We had first a division algebra $\mathscr{V}$ of rank hs^2 over $\mathbb{Q}$, with centre $\mathfrak{R}$ of degree *h* over $\mathbb{Q}$ and carrying a positive involution. Further $(\mathscr{M})$ was upto equivalence over $\mathbb{Q}$, a *q*-fold multiple of $(\mathscr{V})$, the rational hs^2-rowed representation **110**

of $\mathscr{V}$. In the algebra $(\mathscr{V})$, we had an involution $D \to \widetilde{D} = F^{-1}\overline{D}'F$ and the matrix $\underset{q}{G}$ defined by

$$\underset{q}{G} = \underset{q}{F}M_0 > 0 \tag{115}$$

was a positive symmetric matrix with M_0 being in $(\mathscr{M})$ such that $\widetilde{M}_0 = \underset{q}{F^{-1}}M_0'F_q$. Further T_0 was a given nonsingular element of $(\mathscr{F})$ (the commutator algebra of $(\mathscr{M})$) for which

$$\widetilde{T}_0 = \underset{q}{F^{-1}}T_0'\underset{q}{F} = -T_0 \tag{116}$$

The matrix A defined by

$$A = \underset{q}{G}T_0 \tag{117}$$

was a nonsingular rational skew-symmetric matrix defining the Resati involution $M \to M^* = A^{-1}M'A$ in $(\mathscr{M})$. Our problem was first to find R-matrices R in $(\underline{\mathscr{F}})$ for which

$$AR = S = S' > 0 \tag{118}$$

(We recall that the matrix A in (118) is a *'principal matrix'* for R). Associated with each such R-matrix R, we had defined an n-rowed Riemann matrix $\mathscr{P}$ of the form (70), uniquely determined by R, upto a left sided complex non-singular factor. We denoted by $\mathfrak{H}$, the set of $\mathscr{P}$ of the form (70) associated in this way. In the sequel, however, we shall denote by $\mathfrak{H}$ the set of R-matrices in $(\underline{\mathscr{F}})$ themselves.

So $\mathfrak{H}$ depends, a priori, on $(\mathscr{M})$, $M_0 \in (\mathscr{M})$ given in (115) and $T_0 \in (\mathscr{F})$ given in (116). Given $(\mathscr{M})$, we shall now see how far $\mathfrak{H}$ is
111 determined by $(\mathscr{M})$. For our subsequent discussion, we shall exclude $\mathscr{V}$ from being of the type of the six exceptional cases mentioned in the statement of Theorem 7. Hence $\mathfrak{H}$ will always contain a R-matrix having $(\mathscr{M})$ as its exact commutator-algebra. Such a R-matrix shall be referred to as a *generic R-matrix*. We now prove

Proposition 14. *Let $\mathfrak{H}$ be the space of R-matrices associated with $(\mathscr{M})$, M_0 and T_0 as above and $\mathfrak{H}_1$ with $(\mathscr{M})$, M_1 and T_1 in a similar manner. Then $\mathfrak{H} = \mathfrak{H}_1$ if $\mathfrak{H} \cap \mathfrak{H}_1$ contains a generic R-matrix.*

Before proving the proposition, we remark that if R in $\mathfrak{H}$ also lies in $\mathfrak{H}_1$, then both $A = \underset{q}{F} M_0 T_0$ and $A_1 = \underset{q}{F} M_1 T_1$ are principal matrices. The following proposition gives the form of all principal matrices for a generic R-matrix $R \in \mathfrak{H}$. It is not hard to extend it also to the case when the R-matrix is not necessarily irreducible.

Proposition 15. *If A is a principal matrix for a generic $R \in \mathfrak{H}$, then any other principal matrix A_1 of R is of the form AM, where M is a positive element of $(\mathscr{M})$ and conversely, $A_1 = AM$ is a principal matrix for R, for every such $M \in (\mathscr{M})$.*

Proof. From (118), we obtain $S = AR = -R'A$, $S_1 = A_1R = -R'A_1$ and therefore $A^{-1}A_1R = RA^{-1}A_1$. But R being generic and $A^{-1}A_1$ being rational, we see that $A^{-1}A_1 = M \in (\mathscr{M})$. In the first place, $M^* = A^{-1}M'A = -A^{-1}M'A' = -A^{-1}A_1' = M$. Further from $S > 0$, and from $SM = \underline{A}RM = \underline{A}MR = S_1 > 0$, we see, by Lemma 2, that the eigenvalues of M are real positive. In other words, $A_1 = AM$ for a positive element M of $(\mathscr{M})$. Conversely, if M is a positive element of $(\mathscr{M})$ $(M = M^*)$, then $A_1 = AM = M'A = -A_1'$ and further $A_1R =$ **112**
$AMR = ARM$ is symmetric and positive by Lemma 2. We now give the □

Proof of Proposition 14. Let R be a generic R-matrix in $\mathfrak{H} \cap \mathfrak{H}_1$. Then, by proposition 15, $A_1 = AM$ for a positive element M in $(\mathscr{M})$. If $R_0 \in \mathfrak{H}$, then $AR_0 > 0$. But now $A_1R_0 = AMR_0 = AR_0M$ is again positive symmetric, using Lemma 2. Thus A_1 is a principal matrix for R_0 and so $R_0 \in \mathfrak{H}_1$. Thus $\mathfrak{H} \subset \mathfrak{H}_1$ and similarly $\mathfrak{H}_1 \subset \mathfrak{H}$ which proves our proposition.

In the set of T_0 of the form (116), we introduce an equivalence relation as follows, namely, two such matrices T_0 are *equivalent* if they differ by a factor $K \in (\mathscr{L})$ which is totally positive. We denote by $[K_0]$ the equivalence class of K_0.

Proposition 16. *If $\mathfrak{H}$ is the space of R-matrices associated with $(\mathscr{M})$, M_0 and T_0 as above, then $\mathfrak{H}$ depends essentially only on $(\mathscr{M})$ and $[T_0]$.*

Proof. Let $\mathfrak{H}_1$ be the space of R-matrices associated with $(\mathscr{M})$, M_1 and KT_0 where K is in $(\mathscr{Z})$ and has positive eigenvalues. We shall show that $\mathfrak{H} = \mathfrak{H}_1$. Let $R \in \mathfrak{H}$. Then we know that $\underset{q}{F} M_0 T_0 R$ is symmetric and positive. If we could show that

$$\underset{q}{F} M_1 K T_0 R = (\underset{q}{F} M_1 K T_0 R)' > 0 \tag{119}$$

it would follow that $\mathfrak{H} \subset \mathfrak{H}_1$ and then taking K^{-1} instead of K, the reverse inclusion would hold leading to $\mathfrak{H} = \mathfrak{H}_1$. To prove (119), we first remark that from $\underset{q}{F} M_0 (\underset{q}{F} M_0)' > 0$, $\underset{q}{F} M_1 = (\underset{q}{F} M_1)' = \underset{q}{F} M_0 M_0^{-1} M_1 < 0$,

113 it follows in view of Lemma 2 that $M_0^{-1} M_1 \in (\mathscr{M})$ has positive eigenvalues. Hence the product $M_0^{-1} M_1 K$ has again positive eigenvalues (since they commute). Now $(\underset{q}{F} M_1 K T_0 R)' = (T_0 R)' K' \underset{q}{F} M_1 = (T_0 R)' \underset{q}{F} K M_1 = (T_0 R)' \underset{q}{F} M_0 M_0^{-1} M_1 K = \underset{q}{F} M_0 T_0 R M_0^{-1} M_1 K = \underset{q}{F} M_1 K T_0 R$. Further since $\underset{q}{F} M_1 K T_0 R$ is symmetric and $\underset{q}{F} M_0 T_0 R > 0$, it follows that $\underset{q}{F} M_1 K T_0 R = \underset{q}{F} M_0 T_0 R M_0^{-1} M_1 K > 0$ by Lemma 2. □

Conversely, if $(\mathscr{M})$, M_1, T_1 lead to the same $\mathfrak{H}$, then we claim $[T_1] = [T_0]$. For, let R be a generic R-matrix in $\mathfrak{H}$. Then $\underset{q}{F} M_0 T_0$ and $\underset{q}{F} M_1 T_1$ are both principal matrices for R and hence by Proposition 15, $M_0 T_0 = M_1 T_1 M$ for a positive element $M \in (\mathscr{M})$ which means $M_0^{-1} M_1 M = T_0 T_1^{-1}$. From Proposition 6, it follows that $T_0 T_1^{-1} = M_0^{-1} M_1 M = K$ in $(\mathfrak{R})$. From $T_0 = -\widetilde{T}_0$, $\widetilde{T}_1 = -T_1$, it follows that $K \in (\mathscr{Z})$. Further from $\underset{q}{F} M_1 = M_1' \underset{q}{F}$, $\underset{q}{F} M_0 = M_0' \underset{q}{F}$, it follows that $(M_0^{-1} M_1)' \underset{q}{F} M_0 = \underset{q}{F} M_0 M_0^{-1} M_1$ i.e. $M_0^{-1} M_1$ is symmetric under the given positive involution in $(\mathscr{M})$. Moreover, by the same arguments as above, $M_0^{-1} M_1$ has positive eigenvalues. Hence $M_0^{-1} M_1$ is a positive element in $(\mathscr{M})$. Since $M_0^{-1} M_1 M = K$ is in the centre, it follows that the positive elements M and $M_0^{-1} M_1$ in $(\mathscr{M})$ commute. Hence $K = K^*$ and further K has all eigenvalues positive. Thus $T_0 T_1^{-1} \in (\mathscr{Z})$ and has all its eigenvalues positive is $[T_0] = [T_1]$.

From Proposition 15, we know that if A is a principal matrix for a generic R in $\mathfrak{H}$, then any other principal matrix $A_1 = AM$ where M is

a positive element of $(\mathscr{M})$. We shall investigate the cases when A_1A^{-1} is always rE where $r > 0$ in $\mathbb{Q}$. This will be indeed true if the only elements $M \in (\mathscr{M})$ for which $M^* = M$ and all the eigenvalues are real and positive and are precisely of the form rE where $r > 0$ and $r \in \mathbb{Q}$, A **114**
necessary condition for this is that $\mathscr{Z} = \mathbb{Q}$. But even if $\mathscr{Z} = \mathbb{Q}$, we know that in the case when $\mathscr{V} = \mathfrak{g}$ or $\mathscr{V}$ is a noncommutative cyclic algebra, there exist positive elements in $(\mathscr{V})$ other than the positive elements in $(\mathbb{Q})$. But in the case when $\mathscr{V} = \mathfrak{H}$, $(\mathscr{Z} = \mathbb{Q})$ is of type (i) or (iv) or $\mathscr{V} = \mathscr{P}$ with $\mathfrak{H} = \mathscr{Z} = \mathbb{Q}$, the only positive elements in $(\mathscr{M})$ are of the form rE with $r > 0$ in $\mathbb{Q}$. Therefore, in these cases, any two principal matrices for $\mathfrak{H}$ differ at most by a positive rational scalar factor.

We now go back to our definition of a multiplier of a Riemann matrix $\mathscr{P}$. We called an *integral* matrix M a multiplier of $\mathscr{P}$ if $\mathscr{P}M = K\mathscr{P}$ for a complex nonsingular K and later we relaxed the condition that M be integral and allowed M to be rational and not necessarily non-singular. We constructed in §6, Riemann matrices $\mathscr{P}$ with the given division algebra $(\mathscr{M})$ as exact algebra of multipliers. The integral matrices M in this representation $(\mathscr{M})$ form an order $(\mathscr{U})$ in $(\mathscr{M})$ and $\mathscr{P}$ admits all elements of $(\mathscr{U})$ as (integral) multipliers. One could ask the more difficult question of constructing Riemann matrices $\mathscr{P}$ with $(\mathscr{U})$ as the exact ring of multipliers. Now, when we say "an integral multiplier of $\mathscr{P}$", it is necessary to mention the specific representation $(\mathscr{M})$. For, an integral matrix M in $(\mathscr{M})$, will not, in general, go into an integral matrix in a $\mathbb{Q}$-equivalent representation $C^{-1}(\mathscr{M})C$. But it is true that $(\mathscr{U})$ will go over into an order in $C^{-1}(\mathscr{M})C$. If C is a unimodular matrix and $C^{-1}(\mathscr{M})C = (\mathscr{M})$, then $C^{-1}(\mathscr{U})C$ will again be equal to $(\mathscr{U})$. In this connexion, it is then of interest to study the mappings $R \to U^{-1}RU$ for $R \in \mathfrak{H}$ and unimodular U. This, as we shall presently see, leads us to the general modular groups associated with $(\mathscr{M})$. **115**

Proposition 17. *Let U be a unimodular matrix such that the mapping $R \to U^{-1}RU$ is a mapping of $\mathfrak{H}$ into itself where $\mathfrak{H}$ is a space of R-matrices associated with $(\mathscr{M})$ as above. Then the mapping $M \to U^{-1}MU$ is an automorphism of $(\mathscr{M})$. Further, the mapping $R \to U^{-1}RU$ is onto $\mathfrak{H}$.*

Proof. Let R be generic in $\mathfrak{H}$. Then $U^{-1}RU \in \mathfrak{H}$ and by the very con-

struction of $\mathfrak{H}$, $U^{-1}RU$ admits elements of $(\mathscr{M})$ as commutators. In other words, the elements of $U(\mathscr{M})U^{-1}$ commute with R. But R is generic and the elements of $U(\mathscr{M})U^{-1}$ are rational so that $U(\mathscr{M})U^{-1} \subset (\mathscr{M})$. By considerations of rank, we see that $U(\mathscr{M})U^{-1} = (\mathscr{M})$, actually. Let $R \in \mathfrak{H}$; then we claim that $R = U^{-1}R_1U$ for some $R_1 \in \mathfrak{H}$. For, the algebra $U^{-1}(\mathscr{M})U$ leads us to another space $\mathfrak{H}_1$ of R-matrices having $U'AU$ for a principal matrix and admitting $(\mathscr{M}) = U^{-1}(\mathscr{M})U$ as algebra of multipliers. But for the generic elements R of $\mathfrak{H}$, $U^{-1}RU$ is again generic and belongs to $\mathfrak{H} \cap \mathfrak{H}_1$. Thus by Proposition 14, $\mathfrak{H} = \mathfrak{H}_1$ and in other words, the mapping $R \to U^{-1}RU$ is onto $\mathfrak{H}$. The proposition is proved. □

From the working above, we see that, for a generic $R \in \mathfrak{H}$, both A and $U'AU$ are principal matrices. Hence by Proposition 15, $U'AU = AM$ for a positive element in $(\mathscr{M})$. Rewriting this, we have (since $U^* = A^{-1}U'A$)

$$U^*U = M, \quad \text{for a positive element} \quad M \in (\mathscr{M}). \tag{120}$$

If U is a unimodular matrix satisfying (120), then it is easy to verify that the mapping $R \to U^{-1}RU$ is a mapping of $\mathfrak{H}$ onto itself and hence $U^{-1}(\mathscr{M})U = (\mathscr{M})$.

116 It is easy to verify that the $2n$-rowed unimodular matrices U satisfying (120) for some positive element $M \in (\mathscr{M})$ constitute a group Γ_0 which is the *most general* form of the *homogeneous modular group of degree n*. The group Γ_0 contains a trivial normal subgroup Δ consisting of all $U \in \Gamma_0$, for which $U^{-1}RU = R$ for every $R \in \mathfrak{H}$. For any $U \in \Gamma_0$, the mappings $R \to U^{-1}RU$ and $R \to (MU)^{-1}RMU$ are the same, whatever be M in Δ. The group Γ_0/Δ is the most general form of the *inhomogeneous modular group of degree n.*

It is trivial to see that for $U \in \Delta$, $UM \in (\mathscr{M})$ for every $M \in (\mathscr{M})$. For, taking a generic $R \in \mathfrak{H}$, $UMR = URM = RUM$, i.e. $UM \in (\mathscr{M})$.

We shall now define two subgroups Γ_1, Γ_2 of Γ_0 such that Γ_1 is of finite index in Γ_0 and Γ_2 is of finite index in Γ_1 and each one of them containing Δ.

Now, under the automorphism $M \to U^{-1}MU$ of $(\mathscr{M})$, the centre $(\mathfrak{R})$ is taken onto itself i.e. $U^{-1}(\mathfrak{R})U = (\mathfrak{R})$. But the centre $\mathfrak{R}$ being an

algebraic number field of finite degree over $\mathbb{Q}$, admits only finitely many automorphisms over $\mathbb{Q}$ and we define Γ_1 to be the subgroup of $U \in \Gamma_0$ which correspond to the identity automorphism of $\mathfrak{R}$. In other words,

$$\Gamma_1 = \left\{ U \in \Gamma_0 \int U^{-1}KU = K, \text{ for every } K \in (\mathfrak{R}) \right\}$$

It is easy to see that Γ_1 is of finite index in Γ_0. Moreover $\Gamma_1 \supset \Delta$; for, if $K \in (\mathfrak{R})$ and $U \in \Delta$, then, by our remark above, $U \in (\mathscr{M})$ and therefore $KU = UK$. We call the group Γ_1, the *homogeneous modular group of degree n in the wide sense* and the quotient group Γ_1/Δ, the **117** *inhomogeneous modular group of degree n in the wide sense.*

If $U \in \Gamma_1$, we see than that the mapping $M \to U^{-1}MU$ of $(\mathscr{M})$ is an automorphism of $(\mathscr{M})$ which is identity on the centre $(\mathfrak{R})$. Thus, by Skolem's Theorem (23), here exists $M_1 \in (\mathscr{M})$ such that for every $M \in (\mathscr{M})$, we have $U^{-1}MU = M_1^{-1}MM_1$ i.e. $UM_1^{-1}M = MUM_1^{-1}$. In other words, $UM_1^{-1} = T_1 \in (\mathscr{F})$, or

$$U = M_1T_1 = T_1M_1 \text{ with } T_1 \in (\mathscr{F}), M_1 \in (\mathscr{M}) \tag{121}$$

The decomposition (121) of $U \in \Gamma_1$ is clearly not unique. Now $U^*U = M_0$ for a positive element $M_0 \in (\mathscr{M})$ and this gives $T_1^*M_1^*M_1T_1 = M_0$ or $T_1^*T_1 = (M_1^{-1})^*M_0M_1^{-1} = M_2$ in $(\mathscr{M})$. Since M_0 is a positive element in $(\mathscr{M})$, so is M_2, by Proposition 12. But since $M_2 \in (\mathscr{M}) \cap (\mathscr{F}) = (\mathfrak{R})$ and since $M_2 = M_2^*$, it is immediate that M_2 represents a totally positive number in $\mathscr{Z}$. Thus, for T_1 in (121), we have

$$T_1^*T_1 = K_1 \text{ totally positive in } (\mathscr{L}) \tag{122}$$

Suppose for $U \in \Gamma_1$, we have two decompositions as in (121), say $U = T_1M_1 = T_2M_2$. Then it is immediate that $T_1 = T_2K$ for some $K \in (\mathfrak{R})$. We now claim that in the decomposition $U = T_1M_1$ as in (121), we can, by replacing T_1, M_1 respectively by T_1K^{-1}, KM_1 with suitable $K \in (\mathfrak{R})$, ensure that KM_1 is integral and furthermore that $T_2 = T_1K^{-1}$ has the following property, namely, *there exists* $d > 0$ *in* $\mathbb{Z}$ *(depending only on* $(\mathscr{M})$ *and not on* T_2*) for which* dT_2 *is integral.* Thus in (121), we can suppose already that M_1 is *integral* and T_1 *if of "bounded denominator"* **118**

(We shall briefly sketch a proof of this fact in a special case. Let $\mathscr{V}$ be an indefinite quaternion algebra over $\mathbb{Q}$ and $q = 1$. Then $\mathscr{V}$ has a splitting field $\mathfrak{Z} = \mathbb{Q}(\sqrt{a})$ with $a < 0$ in $\mathbb{Z}$. For a element $\delta = \xi + \eta j \in \mathscr{V}$ with $\xi, \eta \in \mathfrak{Z}$ and $j^2 = b(> 0)$ in $\mathbb{Z}$, we have the representation $(\mathscr{M})$ of $\mathscr{V}$ given by $\delta \to M = K_1[D\ \overline{D}]K_1^{-1}$ where $D = \begin{pmatrix} \xi & \eta \\ b\overline{\eta} & \overline{\xi} \end{pmatrix}$, $P_1 = \begin{pmatrix} 1 & 1 \\ \sqrt{a} & -\sqrt{a} \end{pmatrix}$, $K_1 = P_1 \times E_2$. The commutator algebra $(\mathscr{F})$ of $(\mathscr{M})$ is precisely the set of $T = K_1 \begin{pmatrix} \lambda E_2 & \mu\mathscr{F} \\ \overline{\mu}\mathscr{F} & \overline{\lambda}E_2 \end{pmatrix} K_1^{-1}$ where $\lambda, \mu \in \mathfrak{Z}$ and $\mathscr{F} = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$. Let $T \in (\mathscr{F})$ be such that

$$TM = U \qquad (*)$$

with $M\varepsilon(\mathscr{M})$ and U, unimodular. In $(*)$, we can suppose that M is integral already, by replacing T, M respectively by $m^{-1}T$, mM for a suitable $m \in \mathbb{Z}$. Let ω_1, ω_2 be a basis over $\mathbb{Z}$ for the integers in $\mathfrak{Z}$. Denote the matrix $\begin{pmatrix} \omega_1 & \overline{\omega}_1 \\ \omega_2 & \overline{\omega}_2 \end{pmatrix}$ by P and P_1P^{-1} by P_2. We can find ν_1, $\nu_2 \in \mathbb{Z}$ such that ν_1P_1, $\nu_1P_1^{-1}$, ν_2P_2, $\nu_2P_2^{-1}$ have elements which are integers in $\mathfrak{Z}$. Since $M = K_1 \begin{pmatrix} D & 0 \\ 0 & \overline{D} \end{pmatrix} K_1^{-1}$ and $U = K_1 \begin{pmatrix} \lambda E_2 & \mu\mathscr{F} \\ \overline{\mu}\mathscr{F} & \overline{\lambda}E_2 \end{pmatrix} K_1^{-1}M$ are both integral, we see that ν_1^2D, $\nu_1^2\lambda D$, $\nu_1^2\mu\mathscr{F}\overline{D}$, $\nu_1^2\overline{D}$ are all integral. Let $\mathscr{G}_1, \ldots, \mathscr{G}_{h_0}$ be *fixed* integral ideals (say, of minimum norm) in the h_0 ideal classes of $\mathfrak{Z}$. Then there exists $\alpha \in \mathfrak{Z}$ and an ideal $\mathscr{G}_\rho (1 \le \rho \le h_0)$ such that $\nu_1^2D = \alpha \begin{pmatrix} \xi_1 & \eta_1 \\ b\overline{\eta}_1 & \overline{\xi}_1 \end{pmatrix}$ and ξ_1, η_1, $b\overline{\eta}_1$, $\overline{\xi}_1$ have the
119 greatest common divisor $\mathscr{G}_\rho$. Define $T_1 = (\nu_1\nu_2)^{-2}K_1 \begin{pmatrix} \lambda\alpha E_2 & \mu\overline{\alpha}\mathscr{F} \\ \overline{\mu}\alpha\mathscr{F} & \overline{\lambda}\overline{\alpha}E_2 \end{pmatrix} K_1^{-1}$ and $M_1 = (\nu_1\nu_2)^2K_1 \begin{pmatrix} \alpha^{-1}D & 0 \\ 0 & \overline{\alpha}^{-1}\overline{D} \end{pmatrix} K_1^{-1}$. It is clear that M_1 is in $(\mathscr{M})$ and is integral; further $T_1M_1 = U$. Moreover, if we define $d = b\nu_1^4\nu_2^2 \prod_{k=1}^{h_0} N(\mathscr{G}_k)$ (where $N(\mathscr{G}_k)$ denotes the norm of $\mathscr{G}_k$ over $\mathbb{Q}$), we see that dT_1 is integral).

Let us denote by Γ_2, the subgroup of $U \in \Gamma_1$ for which there is a decomposition of the form (121) with unimodular T_1 and M_1 in $(\mathscr{F})$ and $(\mathscr{M})$ respectively. We now prove

Proposition 18. *The group* Γ_2 *is of finite index in* Γ_1.

Proof. Let U_1, U_2 be in Γ_1 and $U_1 = T_1M_1$, $U_2 = T_2M_2$ be the decompositions of U_1, U_2 as in (121). Now, as we remarked, M_1, M_2 may be

supposed to be integral. We shall now prove that if $M_1 \equiv M_2 \pmod{d}$, then $U_2^{-1}U_1 \in \Gamma_2$. Since the number of residue classes of $2n$-rowed integral square matrices modulo d, is finite, it will follow that Γ_2 is of finite index in Γ_1. So let

$$M_1 \equiv M_2 \pmod{d} \tag{123}$$

It is clear that $dM_1^{-1} = dU_1^{-1}T_1$ and $dM_2^{-1} = dU_2^{-1}T_2$ are integral. But from (123), we have $dE_{2n} \equiv dM_2M_1^{-1} \pmod{d}$ which means that $M_2M_1^{-1}$ is integral. In a similar way, $M_1M_2^{-1}$ is also integral so that $M_2 = WM_1$ with unimodular W. But now $U_2U_1^{-1} = T_2M_2M_1^{-1}T_1^{-1} = T_2T_1^{-1}W$ so that $T_2T_1^{-1}$ is itself unimodular in $(\mathscr{F})$. Thus $U_2U_1^{-1}$ is in Γ_2 which is what we sought to prove.

If $U \in \Delta$, then $U \in (\mathscr{M})$ and therefore $\Delta \subset \Gamma_2$. □

We define now another group $\dot{\Gamma}_2$ consisting of unimodular matrices **120**
$T_1 \in (\mathscr{F})$ for which $T_1^*T_1 = K$ which represents a totally positive unit in $\mathscr{L}$. It is clear that $\dot{\Gamma}_2 \subset \Gamma_2$. Defining $\dot{\Delta}_2$ as the subgroup of $\dot{\Gamma}_2$ consisting of unimodular $U \in (\mathfrak{R})$, we see that $\dot{\Delta}_2 \subset \Delta$.

Any $U \in \Gamma_2$ is of the form T_1M_1 with unimodular T_1 in $(\mathscr{F})$ satisfying (122) and unimodular M_1 in $(\mathscr{M})$. Since T_1 and T_1^* in this decomposition commute, we get, by iteration,

$$(T_1^*)^{-1}T_1^1 = (T_1^1)^*T_1^1 = K_1^1 \tag{124}$$

for every positive integer l. Now although T_1 is unimodular, T_1^* is not necessarily integral so that K_1 is not necessarily integral. But since dT_1^l is integral and A is fixed, we see that K_1^l is of bounded denominator for every $l > 0$, from (124). This is impossible, unless K_1 represents an integer in $(\mathscr{Z})$. By the same argument, we can show that K_1 is integral so that K_1 is actually a (totally positive) unit in $(\mathscr{Z})$. Thus for $U = T_1M_1 \in \Gamma_2$ with $T_1 \in (\mathscr{F})$, we see first that $T_1 \in \dot{\Gamma}_2$ and furthermore, for any $T_1 \in \dot{\Gamma}_2$.

$$T_1^*T_1 = K_1, \text{ a totally positive } \textit{unit} \text{ in } (\mathscr{Z}) \tag{125}$$

We construct a mapping ψ of Γ_2 into $\dot{\Gamma}_2/\dot{\Delta}_2$ by defining $\psi(U) =$ the coset of $\dot{\Gamma}_2$ modulo $\dot{\Delta}_2$ containing T_1 where T_1 in $(\mathscr{F})$ occurs in

the decomposition $U = T_1 M_1$. It is clear that ψ is well-defined, for if $U = T_1 M_1 = T_2 M_2$, then $T_2^{-1} T_1 \in \dot{\Delta}_2$ by using (125). Further clearly ψ is a homomorphism of Γ_2 onto $\dot{\Gamma}_2/\dot{\Delta}_2$, the kernal being exactly Δ. Thus we have proved that

$$\Gamma_2/\Delta \textit{ is isomorphic to } \dot{\Gamma}_2/\dot{\Delta}_2$$

121 The group $\dot{\Gamma}_2/\dot{\Delta}_2$ is referred to as the *inhomogeneous modular group of degree n.*

Finally, we define the group $\dot{\Gamma}_3$ as the subgroup of $T \in \dot{\Gamma}_2$ for which

$$T^* T = E \tag{126}$$

and $\dot{\Delta}_3$ as the subgroup of K in $\dot{\Gamma}_3$ for which $K \in (\mathfrak{R})$. It is easy to see that $\dot{\Delta}_3$ is precisely the set of roots of unity in $(\mathscr{F})$ which belong to the order $(\mathscr{U})$ in $(\mathscr{M})$ and therefore, $\dot{\Delta}_3$ is finite. Although, in view of (117), the definition (126) of $\dot{\Gamma}_3$ apparently depends on $\underset{q}{G}$, it is trivial to verify that (126) depends only on $\underset{q}{F}$.

Proposition 19. *The group* $\dot{\Gamma}_3/\dot{\Delta}_3$ *is of finite index in* $\dot{\Gamma}_2/\dot{\Delta}_2$.

Proof. Let $\mathscr{E}$ be the group of all totally positive units in $(\mathscr{Z})$, $\mathscr{E}_1 = \mathscr{E} \cap (\mathscr{U})$ and $\mathscr{E}_2$, the group of squares of elements in $\mathscr{E}_1$. By Dirichlet's theorem on units in algebraic number fields, there exist finitely many elements $L_1, \ldots, L_a$ of $\mathscr{E}$ such that any K in $\mathscr{E}$ is of the form $K = NL_\nu$ for some $N \in \mathscr{E}_2$ and some L_ν. Let now $T_1 \in \dot{\Gamma}_2$ satisfy (125) and let $K_1 = N_1^2 L_\nu$ for some $N_1 \in \mathscr{E}_1$ and some L_ν. Thus

$$(N_1^{-1} T_1)^* (N_1^{-1} T_1) = L_\nu \tag{127}$$

On the other hand, let A_ν unimodular in $(\mathscr{F})$ be a fixed matrix satisfying $A_\nu^* A_\nu = L_\nu$, for $1 \le \nu \le a$. Then clearly $N_1^{-1} T_1 A_\nu^{-1} \in \dot{\Gamma}_3$ i.e. $T_1 = N_1 B A_\nu$ for $N_1 \in (\mathscr{Z})$, $B \in \dot{\Gamma}_3$ and one of the finitely many matrices $A_1, \ldots, A_a$. It is immediate using (127) that $\dot{\Gamma}_3/\dot{\Delta}_3$ is of finite index in $\dot{\Gamma}_2/\dot{\Delta}_2$. □

122 The group $\dot{\Gamma}_3$ is called the *homogeneous modular group of degree n in the restricted sense.* The quotient $\dot{\Gamma}_3/\dot{\Delta}_3$ is the *inhomogeneous modular group in the restricted sense.*

The groups $\dot{\Gamma}_2/\dot{\Delta}_2$ and $\dot{\Gamma}_3/\dot{\Delta}_3$ occur in the literature already in special cases.

In face, taking $\mathscr{V} = \mathfrak{R}$, a totally real field over $\mathbb{Q}$, $q = 2$ and with obvious restrictions on $(\mathscr{M})$ we see that they are nothing but the inhomogeneous Hilbert modular group over $\mathfrak{R}$, in the wide sense and in the narrow sense respectively.

It might be of interest to construct fundamental regions for these groups in $\mathfrak{H}$ and study the automorphic functions on $\mathfrak{H}$ relative to these groups. We refer the interested reader to some recent work of K.G. Ramanathan (15) in this direction.

We might conclude with an outline of a method of constructing a fundamental region in the $\mathfrak{H}$-space, for one of the groups above, say $\dot{\Gamma}_3$. The group $\dot{\Gamma}_3$ acts on $\mathfrak{H}$ as follows; namely, to $T \in \dot{\Gamma}_3$ corresponds the mapping $R \to T^{-1}RT$ of $\mathfrak{H}$ onto itself. Let A be a principal matrix for $\mathfrak{H}$. We simplify our problem by considering the matrices $AR = S = S' > 0$ (for $R \in \mathfrak{H}$). In terms of S, the mapping $R \to T^{-1}RT$ is just the mapping $S \to T'ST$. By Minkowski's "reduction theory" for unimodular matrices acting on the space of $2n$-rowed real symmetric positive-definite matrices, we know that corresponding to the given S, there exists a unimodular matrix T such that $S_1 = T'ST$ lies in the "reduced" Minkowski domain $\mathscr{F}_{2n}$. But T may not belong to **123** $\dot{\Gamma}_3$. On the other hand, we know that $R^2 = -E_{2n}$ i.e. $A^{-1}SA^{-1}S = -E_{2n}$ i.e. $A'S^{-1}A = S$ i.e. $(T'AT)'S_1^{-1}(T'AT) = S_1$. Again, since S_1 is "reduced" in the sense of Minkowski, we conclude by a theorem of Siegel (Satz 5, p.200 [20]) that $T'AT$ belongs to a finite set of matrices, say $T_1'AT_1, T_2'AT_2, \ldots, T_\mu'AT_\mu$. Now, for any "reducing" matrix T obtained as above, we have $T'AT = T_k'AT_k$ for some

$$T_k (1 \leq k \leq \mu). \textit{i.e.}\ (TT_k^{-1})'A(TT_k^{-1}) = A.$$

In other words, $(TT_k^{-1})^*(TT_k^{-1}) = E$ i.e. $TT_k^{-1} \in \dot{\Gamma}_3$. It may now be

verified as usual that

$$\mathscr{F} = \bigcup_{k=1}^{\mu} (A^{-1} T'^{-1}_k \mathscr{F}_{2n} T_k^{-1} \cap \mathfrak{H})$$

is a fundamental region for $\dot{\Gamma}_3$ in the $\mathfrak{H}$-space.

Bibliography

124

[1] A.A. Albert : Structure of Algebras, New York, 1939.

[2] —— : On the construction of Riemann matrices *I*, Ann. of Math., pp.1-28, Vol.35 (1934).

[3] —— : A solution of the principal problem in the theory of Riemann matrices, Ann. of Math., pp. 500-515, Vol.35 (1934).

[4] —— : On the construction of Riemann matrices II, Ann. of Math. pp.376-394, Vol.36 (1935).

[5] —— : Involutorial simple algebras and real Riemann matrices, Ann. of Math., pp.886-964 Vol. 36 (1935).

[6] —— : On involutorial algebras, Proc. Nat.Acad. Sci. U.S.A., pp.480-482, Vol.41, (1955).

[7] R. Brauer, H. Hasse and E. Noether : Beweis eines Hauptsatzes in der Theorie der Algebren, Crelle's Journal, pp.399-404, vol.167 (1931).

[8] M. Deuring : Algebren, Chelsea, 1948.

[9] H. Hasse : Theory of cyclic algebras over an algebraic number field, Trans. A.M.S., pp.170-214, Vol.34 (1932).

[10] G. Humbert : Sur les fonctions abéliennes singulières, Oeuvres, pp.297-498, t.II, 1936.

[11] S. Lefschetz : On certain numerical invariants of algebraic varieties with applications to abelian varieties, Trans. A.M.S., pp.327-482, Vol.22 (1921). **125**

[12] H. Poincaré : Sur la réduction des intégrales abéliennes, Oeuvres, pp.333-351, t.III, 1934.

[13] I.I. Pyatetskii-Shapiro : Singular Modular functions, Izv. Akad. Nauk SSSR, Ser. mat. pp.53-98, Vol.20 (1956) (also A.M.S. Translations, Ser. 2., pp.13-58, Vol.10 (1956)).

[14] —— : Theory of modular functions and related questions in the theory of discrete groups, Uspekhi Math. Nauk, pp.99-136, Tom. XV, No.1 (1960). (also Russian Math. Surveys, pp.97-128, Vol.XV (1960)).

[15] K.G. Ramanathan : Quadratic forms over involutorial division algebras II, Math. Ann. pp.293-332, Bd. 143 (1961).

[16] B. Riemann : Theorie der abelschen Funktionen, Gesamm. Math. Werke, pp.88-142, Dover, 1953.

[17] C.Rosati : Sulle matrici di Riemann, Rend. Circ. Mat. Palermo, pp.79-134, t.53 (1929).

[18] G. Scorza : Intorno alla teoria generale delle matrici di Riemann, Rend. Circ. Mat. Palermo, pp.263-380, t.41 (1916).

126 [19] C.L. Siegel : Darstellung total positiver Zahlen durch Quadrate, Math. Zeit. pp.246-275, Bd.11(1921).

[20] —— : Einheiten quadratischer Formen, Abh. math. Sem. Hans. Univ., pp.209-239, Bd. 13(1940).

[21] —— : Discontinuous groups, Ann. of Math., pp.674-689, Vol.44 (1943).

[22] —— : Die Modulgruppe in einer einfachen involutorischen Algebra, Festschrift Akad. Wiss. Göttingen, 1951.

[23] T. Skalem : Zur Theorie der assoziativen Zahlensysteme, Skr. Norske Vid. - Akad., Oslo, pp.21-22, 1927.

[24] J.H.M. Wedderburn : On division algebras, Trans. A.M.S., pp.129-135, Vol. 22(1921).

[25] A. Weil : Algebras with involutions and the classical groups, Jour. Ind. M.S., pp.589-623, Vol.24 (1960).

[26] —— : Introduction à l'étude des variétés kählériennes, Hermann, 1958.

[27] H. Weyl : On generalized Riemann matrices, Ann. of Math. pp.714-729, Vol. 35 (1934).

[28] —— : Generalized Riemann matrices and factor sets, Ann. of Math. pp.709-745, Vol.37(1936).