ANNALS OF MATHEMATICS
Vol. 37, No. 3, July, 1936

GENERALIZED RIEMANN MATRICES AND FACTOR SETS

BY HERMANN WEYL

(Received January 22, 1936)

INTRODUCTION

(for the expert only!)

Led by a normalization of integrals of the first kind on a Riemann surface, differing from Riemann's own method in its independence of any dissection of the surface, I suggested in a previous note[1] a natural generalization of the classical concept of Riemann matrices, and expressed the hope that it would tend to simplify considerably the "existential" part in the establishment of necessary and sufficient conditions. The present paper claims to bear out this promise; it contains a complete and simple solution of the problem in terms of "factor sets." This is another point that I had in mind when I drafted the first note: suspicion that it might not be wise under all circumstances to restrict oneself to Galois splitting fields (and thus to sacrifice the minimum degree) induced me to adopt R. Brauer's factor sets in an arbitrary splitting field rather than E. Noether's crossed products over a Galois field. The whole subject is here given a new twist in replacing the study of the commutator algebra $\mathfrak{A}$ of a Riemann matrix R by what I call the associated rational algebra $\mathfrak{L}$; it has the same rational commutator algebra $\mathfrak{A}$ as R and its closure in the field of all real numbers contains R. This change of view was suggested to me by the fact that in the Schur-Brauer theory, construction of splitting fields for a simple algebra $\mathfrak{L}$ is tied up with the maximum subfields of its commutator algebra $\mathfrak{A}$ rather than of $\mathfrak{L}$ itself. Reward in the form of further simplification appears to confirm the new standpoint as a better start for the attack on our problem. To make the paper as easy reading as possible its larger part is devoted to a proof-documented restatement of the foundations,—including the classical facts about simple algebras and the more elementary parts of the Schur-Brauer theory of factor sets.

A. A. Albert's new thorough investigation of the subject[2] unfolding all its aspects and culminating in a complete structural analysis of the commutator algebras of generalized Riemann matrices (Theorems 27–30 on pp. 917–919)

[1] "On generalized Riemann matrices," *Annals of Math.* **35** (1934), pp. 714–729.—Corrigendum: The formula $\check{P}_{\alpha\beta} = y_{\alpha\beta}P_{\alpha\beta}$ at the end of the last line on p. 724 should read: $C_\alpha^{-1}\check{P}_{\alpha\beta}C_\beta = y_{\alpha\beta}P_{\alpha\beta}$.

[2] *Annals of Math.* **36** (1935), pp. 886–964.—Albert does me the honor of associating my name with the kind of matrices under investigation; but would it not be better, if a proper name is to be attached to them, to stand by the former designation as Riemann matrices —even at the expense of having to add an adjective like "generalized"?

prompted me to resume my own line of approach. Though independent in other regards, I borrow from him one essential remark: that apart from a relatively harmless adjunction, the splitting field is totally real; it follows immediately from Rosati's theorem contending that the roots of an "even" matrix of the commutator algebra $\mathfrak{A}$ are real. Its former application to the centrum only was not exhaustive enough. The "harmless" adjunction consists either of nothing, or of a square root, or a quaternion. So it seems natural to distinguish three cases instead of making the old discrimination between "first and second kind" which referred to the character of the centrum.

[Paragraphs included in bold-face square brackets **[ ]** are of minor importance or interrupt the main trend of thought.]

1. Matrix Algebras and their Commutators

(1.1) Let a reference field k be given. A *linear k-set* or *vector-space in k* consists of elements that allow addition and multiplication by numbers in k. n elements $e_1, \cdots, e_n$ such that each element x is expressible as a linear combination

$$x = \xi_1 e_1 + \cdots + \xi_n e_n \qquad (\xi_i \text{ in } k)$$

in a unique manner form a *base* or a coordinate system; the numbers ξ_i are the coordinates of x. The number n is called the *order* of our linear set $\mathfrak{l}$, or the dimensionality of the vector space.

$\mathfrak{l}$ is a *k-algebra* if multiplication of its elements is added to the list of permissible operations.

A square matrix

$$A = \| \alpha_{ij} \| \qquad (i, j = 1, \cdots, g)$$

of g rows and columns is called of *degree g*; the same name applies to a set $\mathfrak{A}$ of matrices A of degree g. A lies in k when all the numbers α_{ij} lie in k. Each such matrix may be interpreted as a linear mapping of a g-dimensional vector space $\mathbf{P}$ on itself. $E = E_g$ denotes the unit matrix of degree g, $A' = \| \alpha_{ji} \|$ the transposed matrix of A. A set $\mathfrak{A} = \{A\}$ goes into an equivalent set if all its mappings A become expressed in a new coordinate system. The set is *irreducible* (in k) if the k-vector space $\mathbf{P}$ contains no linear subspace invariant under all the transformations A of $\mathfrak{A}$, other than 0 and $\mathbf{P}$ itself. $\mathfrak{A}$ is *linearly* or *algebraically closed in k* provided its elements A form a linear k-set or a k-algebra respectively. Any given set $\mathfrak{A}$ gives rise to a linear or algebraic k-closure: the smallest linear k-set, or k-algebra of matrices containing all the members A of $\mathfrak{A}$; it is easy to describe how to construct them if a base of $\mathfrak{A}$ is given. By looking upon the members A of an algebraically closed set $\mathfrak{A}$ as abstract elements allowing addition and multiplication among each other and multiplication by numbers in k, the set $\mathfrak{A}$ changes into an abstract algebra $\mathfrak{a}$ with elements a of which $\mathfrak{A}$; $a \rightarrow A$ is a faithful representation. We shall stick to this convention throughout, that corresponding types like A and a, $\mathfrak{A}$ and $\mathfrak{a}$ of the upper case and the lower case are used to mark the transition from matrices to abstract elements. In general, a correspondence $a \to T(a)$ established between the elements a of an algebra $\mathfrak{a}$ and matrices $T(a)$ in k of degree g is called a *k-representation* of $\mathfrak{a}$ provided it preserves the fundamental operations:

$$T(a + b) = T(a) + T(b) \; ; \qquad T(\lambda a) = \lambda \cdot T(a) \; ; \qquad T(ab) = T(a) \cdot T(b)$$

$$(a, b \text{ elements in } \mathfrak{a} \,, \qquad \lambda \text{ a number in } k) \,.$$

The representation is *faithful* if different elements a are represented by different matrices $T(a)$. The *regular representation* $(\mathfrak{a})$: $a \to (a)$ associates with the element a of $\mathfrak{a}$ the mapping

$$(a): \quad x \to x' = ax$$

whose argument x varies over $\mathfrak{a}$; its representation space is thus $\mathfrak{a}$ itself considered as an h-dimensional vector space $\mathfrak{o}$; its degree is the order h of $\mathfrak{a}$.

A linear k-set or a k-algebra $\mathfrak{A}$ of matrices may be closed in or *extended* to a field K over k; if $e_i (i = 1, \cdots, h)$ is a basis of the set the extended K-set or K-algebra consists of all sums $\sum_i \xi_i e_i$ in which now the components ξ_i vary over K. This operation can thus be described in terms of the abstract scheme $\mathfrak{a}$ (in the case of an algebra, the multiplication table of the e_i is preserved). The extension is denoted by $\mathfrak{A}_K$, $\mathfrak{a}_K$ respectively.

The matrix A is a *commutator* of a given matrix set $\mathfrak{L}$ if it commutes with every member L of $\mathfrak{L}$:

$$AL = LA \,.$$

Those commutators A that lie in a field k form a k-algebra $\mathfrak{A}$ of matrices, the *commutator algebra* in k.

A k-algebra $\mathfrak{A}$ of matrices A in k (or its abstract scheme $\mathfrak{a}$) is a *division algebra* when all its matrices A are non-singular: $\det A \neq 0$, with the exception only of $A = 0$. According to Schur's lemma, a matrix A in k that commutes with all matrices of a k-irreducible set $\mathfrak{L}$ is either 0 or non-singular; hence *the commutator algebra $\mathfrak{A}$ in k of the irreducible $\mathfrak{L}$ is a division algebra.* Proof: the columns of the commutator A when considered as vectors span an invariant subspace.

A set $\mathfrak{A}$ of matrices A in k, when irreducible and algebraically closed in k, or its abstract counter-image $\mathfrak{a}$, is called *simple*. A simple algebra $\mathfrak{a}$ shall thus always be defined by means of its faithful irreducible representation $\mathfrak{A}$.

We exclude throughout this section any "degenerate" matrix algebra $\mathfrak{A}$ (or representation) whose matrices A map the total vector space upon the same *proper* linear subspace.

(1.2) About division and simple algebras we remind the reader of the following propositions whose proofs shall here be arranged in as elementary a way as possible and according to two principles: first, the matrix algebras are considered the primary subject, the abstract schemes merely as secondary tools to facilitate their management; second, we shun the somewhat unpleasant "radicals" (there are none in our matrix communities—so why talk about them?).

The terms "matrix," "algebra," "irreducible" refer to a given number field k throughout, and thus mean "matrix in k," "k-algebra" and "irreducible in k."

THEOREM (1.2-A). *A division algebra* $\mathfrak{a}$ *is characterized by these two properties: it contains a unit element* e (satisfying $xe = ex = x$ for all x in $\mathfrak{a}$), *and every element* a *except* 0 *has an inverse* a^{-1}: $a \cdot a^{-1} = a^{-1} \cdot a = e$.

The regular representation $(\mathfrak{a})$ *of* $\mathfrak{a}$ *is faithful as well as irreducible, and hence* $\mathfrak{a}$ *is simple. Each representation* $a \to A(a)$ *is a multiple* t *of* $(\mathfrak{a})$, i.e. in an appropriate coordinate system common to all elements a, the matrix $A(a)$ decomposes into t matrices (a) along the main diagonal.

PROOF. A matrix A of degree g has its characteristic polynomial

$$\varphi(z) = \det(zE - A) = z^g + \alpha_1 z^{g-1} + \cdots + \alpha_g .$$

A itself satisfies the equation

$$\varphi(A) \equiv A^g + \alpha_1 A^{g-1} + \cdots + \alpha_{g-1} A + \alpha_g E = 0 .$$

When A is non-singular, the last coefficient α_g is $\neq 0$. Hence a matrix algebra $\mathfrak{A}$ containing a non-singular element A involves E and the inverse matrix A^{-1} of A:

$$E = -\frac{1}{\alpha_g}(A^g + \alpha_1 A^{g-1} + \cdots + \alpha_{g-1} A),$$

$$A^{-1} = -\frac{1}{\alpha_g}(A^{g-1} + \alpha_1 A^{g-2} + \cdots + \alpha_{g-1} E) .$$

This remark shows that a division algebra possesses the two properties mentioned in the first paragraph of our theorem after we once and for all have excluded the "trivial case" of the zero-algebra consisting of the one matrix 0.

Vice versa: let $\mathfrak{a} = \{a\}$ have these two properties. We represent a by the linear mapping

$$(a): \quad x \to x' = ax .$$

The terms invariant, irreducible, in the space $\mathfrak{o}$ of the regular representation, shall always refer to the set $(\mathfrak{a})$ of all these transformations (a). In our case the equation $x' = ax$ $(a \neq 0)$ establishes a one-to-one correspondence $x \to x'$ (inversion $x = a^{-1}x'$) and hence (a) is non-singular. The regular representation is faithful since (a) and (b) carry the unit element e into two different elements $ae = a$ and $be = b$ if $a \neq b$. Hence, in replacing $\mathfrak{a}$ by the matrix algebra $(\mathfrak{a})$, our original definition of a division algebra is fulfilled.

$(\mathfrak{a})$ is irreducible. An invariant subspace of $\mathfrak{o}$ when containing a single element $i \neq 0$ necessarily involves all elements of form ai (a in $\mathfrak{a}$) and hence every element b of $\mathfrak{a}$ whatsoever ($a = b \cdot i^{-1}$). This proves $\mathfrak{a}$ to be simple.

Suppose, finally, we are given an arbitrary representation $a \to A = A(a)$ of $\mathfrak{a}$ in an n-dimensional vector space $\mathbf{P}$ whose generic vector is denoted by $\mathfrak{x}$ and which we span by a coordinate system $\mathfrak{e}_1, \cdots, \mathfrak{e}_n$. The terms invariant, irreducible, when applied to subspaces of $\mathbf{P}$, refer to the algebra $\mathfrak{A}$ of matrices A.

An equation $\mathfrak{x}' = a\mathfrak{x}$ is to be interpreted as meaning $\mathfrak{x}' = A(a)\mathfrak{x}$. Let $\mathbf{P}_i$ be the subspace consisting of all vectors $\mathfrak{x} = x\mathfrak{e}_i$, one obtains when x varies over $\mathfrak{a}$. The correspondence $x \rightarrow \mathfrak{x}$ thus established is a similarity, i.e. ax goes into $a\mathfrak{x}$; hence $\mathbf{P}_i$ is invariant under the transformations A of $\mathfrak{A}$. Either $\mathbf{P}_i$ is zero or this mapping of $\mathfrak{o}$ on $\mathbf{P}_i$ is a one-to-one correspondence. Indeed, the elements x for which $x\mathfrak{e}_i = 0$ form an invariant subspace of $\mathfrak{o}$; and as $(\mathfrak{a})$ is irreducible, either every x or no x except zero, satisfies $x\mathfrak{e}_i = 0$. (This "typical argument" recurs again and again.) In taking up the subspaces $\mathbf{P}_1, \cdots, \mathbf{P}_n$ one after the other, a $\mathbf{P}_i$ is either contained in the sum of the preceding ones, or linearly independent of them; this fact is just another application of the typical argument. By dropping a term $\mathbf{P}_i$ in the first case one reduces our sequence $\mathbf{P}_1, \cdots, \mathbf{P}_n$ to a decomposition of $\mathbf{P}$ into linearly independent irreducible invariant subspaces in each of which $\mathfrak{A}$ induces a representation equivalent to $(\mathfrak{a})$.

THEOREM (1.2-B). *A simple algebra* $\mathfrak{a}$ *contains a unit element. Its regular representation is a multiple t of that faithful irreducible representation* $\mathfrak{A}$: $a \rightarrow A$ *through which* $\mathfrak{a}$ *was defined. The order h is a multiple of the degree g*: $h = gt$.

The matrices A of degree g are linear mappings in a g-dimensional vector space $\mathbf{P}$. The regular representation $(\mathfrak{A})$ associates with A the linear mapping

$$(A): \quad X \rightarrow X' = AX$$

whose argument X varies within the linear set $\mathfrak{A}$ that here appears as an h-dimensional vector space $\mathfrak{o}$. Let us pick out an irreducible invariant subspace $\mathfrak{o}_1$ of $\mathfrak{o}$. $\mathfrak{o}_1$ is similar to $\mathbf{P}$ under their respective transformations (A) and A. Indeed, let A^0 be an element $\neq 0$ in $\mathfrak{o}_1$ and $\mathfrak{e}$ a vector in $\mathbf{P}$ such that $A^0\mathfrak{e} \neq 0$. The formula $\mathfrak{x} = X\mathfrak{e}$ (X in $\mathfrak{o}_1$) maps $\mathfrak{o}_1$ on an invariant subspace $\mathfrak{o}_1\mathfrak{e}$ of $\mathbf{P}$ by the similarity $X \rightarrow \mathfrak{x}$; for $X \rightarrow \mathfrak{x}$ entails $AX \rightarrow A\mathfrak{x}$. The subspace $\mathfrak{o}_1\mathfrak{e}$ is either zero or the whole space $\mathbf{P}$, because of the irreducibility of $\mathfrak{A}$. The first possibility is here excluded by $A^0\mathfrak{e} \neq 0$. In the remaining case the similarity $X \rightarrow \mathfrak{x}$ is a one-to-one correspondence between $\mathfrak{o}_1$ and $\mathbf{P}$ due to the irreducibility of $\mathfrak{o}_1$. This proves that any irreducible part of $(\mathfrak{A})$ is equivalent to the representation $\mathfrak{A}$. There exists an element I_1 in $\mathfrak{o}_1$ such that $\mathfrak{e} = I_1\mathfrak{e}$. Because of the invariance of $\mathfrak{o}_1$, the matrix XI_1 lies in $\mathfrak{o}_1$ for every matrix X in $\mathfrak{o}$; since both matrices X and XI_1 change $\mathfrak{e}$ into the same vector $\mathfrak{x} = X\mathfrak{e}$ they must coincide for an X lying in $\mathfrak{o}_1$; in particular $I_1I_1 = I_1$. The formula

$$X = XI_1 + (X - XI_1) = X_1 + Y_1$$

decomposes $\mathfrak{o}$ into two independent invariant subspaces: $\mathfrak{o}_1$ with the idempotent generator I_1, and a remainder $\mathfrak{o}_1^*$ consisting of all matrices of the form $Y_1 = X - XI_1$. The elements X_1 and Y_1 of $\mathfrak{o}_1$ and $\mathfrak{o}_1^*$ obey the relations $X_1I_1 = X_1$, $Y_1I_1 = 0$, respectively. Continuation of this process leads to the decomposition of the regular representation into irreducible parts each of which is equivalent to the representation $\mathfrak{A}$:

$$X_1 = XI_1, \qquad Y_1 = X - XI_1; \qquad X_2 = Y_1I_2^*, \qquad Y_2 = Y_1 - Y_1I_2^*;$$

and so on. Hence the regular representation $(\mathfrak{a})$ is a multiple t of $\mathfrak{A}$ and $h = tg$.

We have constructed the decomposition $\varrho = \varrho_1 + \varrho_2 + \cdots + \varrho_t$:

$$X = X_1 + X_2 + \cdots = XI_1 + (X - XI_1)I_2^* + \cdots$$
$$= XI_1 + XI_2 + \cdots ;$$
$$I_1 = I_1, \qquad I_2 = I_2^* - I_1 I_2^*, \cdots .$$

As XI_α is the component X_α of X lying in ϱ_α we have

$$I_\beta I_\alpha = 0 \text{ for } \beta \neq \alpha, \qquad I_\alpha I_\alpha = I_\alpha .$$

The sum

$$I = I_1 + I_2 + \cdots + I_t$$

satisfies the equation $XI = X$(X in $\mathfrak{A}$), in particular $II = I$. All vectors $\mathfrak{y}$ carried by I into zero: $I\mathfrak{y} = 0$, form an invariant subspace of $\mathbf{P}$ because of

$$X\mathfrak{y} = XI\mathfrak{y} = 0 \qquad (X \text{ in } \mathfrak{A}).$$

Hence either all vectors $\mathfrak{y}$ fulfill this equation, or the vector $\mathfrak{y} = 0$ only. The first possibility would result in the trivial case once and for all excluded. Since $\mathfrak{y} = \mathfrak{x} - I\mathfrak{x}$ satisfies the equation $I\mathfrak{y} = 0$, the other alternative leads to the identity $\mathfrak{x} = I\mathfrak{x}$, proving I to be the unit matrix E.

One may add to our theorem the statement that *every k-representation of $\mathfrak{a}$ decomposes into irreducible parts equivalent to the representation $\mathfrak{A}$.* This is an immediate consequence of the general proposition:

THEOREM (1.2-C). *If the regular representation* ($\mathfrak{a}$) *of an algebra $\mathfrak{a}$ decomposes into irreducible parts $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\cdots$, then every representation decomposes into parts each of which is equivalent to one of the $\mathfrak{A}_i$.*

PROOF: We assumed that $\mathfrak{a}$, considered as the space ϱ of the regular representation, decomposes into irreducible invariant subspaces $\varrho_1, \varrho_2, \cdots , \varrho_t$. Let $\mathfrak{x}$ be the generic vector and $\mathfrak{e}_1, \cdots , \mathfrak{e}_g$ a coordinate system of the space $\mathbf{P}$ of the given representation

$$\mathfrak{A}\colon \; a \to A = A(a).$$

Again, $\mathfrak{x}' = a\mathfrak{x}$ shall mean $\mathfrak{x}' = A(a)\mathfrak{x}$ and $\varrho_\alpha \mathfrak{e}$ denotes the set of all vectors $\mathfrak{x} = x\mathfrak{e}$ (x in ϱ_α). We then form the table

$$\varrho_1\mathfrak{e}_1, \cdots , \varrho_t\mathfrak{e}_1,$$
$$\varrho_1\mathfrak{e}_g, \cdots , \varrho_t\mathfrak{e}_g .$$

Going through it as one reads the words in a book, and applying essentially the same argument as in the case of the division algebra, we obtain the sought-for decomposition of $\mathbf{P}$.

(1.3) We now pass to the relationship of this analysis to the commutator idea. It springs from the following source:

THEOREM (1.3-A). *If the algebra $\mathfrak{a}$ contains a unit element e, the only linear* *transformations that commute with all transformations* $(a)\colon x \rightarrow x' = ax$ *are of the form* $x \rightarrow y = xb$ *(b an element in* $\mathfrak{a}$*).*

Indeed, if $y = B(x)$ is such a commutator, we must have by definition

$$B(ax) = a \cdot B(x). \tag{1.31}$$

Put $B(e) = b$ and apply (1.31) to $x = e$: one thus gets the formula desired, $B(a) = ab$, for every a.

When we designate by $\mathfrak{a}'$ the *inverse algebra* of $\mathfrak{a}$ differing from $\mathfrak{a}$ in that the product of two elements a and b is now defined as ba rather than ab, we may express our result thus: *The commutator algebra of the regular representation of* $\mathfrak{a}$ *is the regular representation of* $\mathfrak{a}'$; the relationship is hence *mutual.*

This applies in particular to a division algebra $\mathfrak{a}$; then both regular representations $(\mathfrak{a})$ and $(\mathfrak{a}')$ are irreducible.

We take up again our *simple algebra* $\mathfrak{A}$ or $\mathfrak{a}$. The commutator algebra $\mathfrak{B}$ of $\mathfrak{A}$ is *in abstracto* a division algebra $\mathfrak{b}$ (of order d), hence *in concreto* a multiple $t(\mathfrak{b})$ of $\mathfrak{b}$'s regular representation $(\mathfrak{b})$: the generic matrix of $\mathfrak{B}$ has the form

$$\left\| \begin{matrix} B & & \\ & \ddots & \\ & & B \end{matrix} \right\| \quad (t \text{ rows})$$

where B varies over all the operators

$$(b)\colon\ x \rightarrow x' = bx \quad (x \text{ variable in } \mathfrak{b})$$

belonging to the elements b of $\mathfrak{b}$. Hence $g = d \cdot t$. The commutator algebra $\mathfrak{A}^*$ of $\mathfrak{B}$ consists of all matrices of the form

$$\left\| \begin{matrix} A_{11} & \cdots & A_{1t} \\ \cdots & \cdots & \cdots \\ A_{t1} & \cdots & A_{tt} \end{matrix} \right\|,$$

where each A_{ik} is an operator

$$x \rightarrow x' = xb \quad (b \text{ in } \mathfrak{b})$$

of the regular representation $(\mathfrak{b}')$ of the inverse division algebra $\mathfrak{b}'$. This we express by the equation

$$\mathfrak{A}^* = (\mathfrak{b}')_t. \tag{1.32}$$

$\mathfrak{A}^*$ evidently contains $\mathfrak{A}$. The fact that *it does not extend beyond* $\mathfrak{A}$ can be established by the following simple indirect argument. Were $\mathfrak{A}^*$ really larger than $\mathfrak{A}$, then the same would be true for any multiple of $\mathfrak{A}$, in particular for the regular representation $(\mathfrak{a})$ of $\mathfrak{a}$ contrary to Theorem (1.3-A), which shows that $(\mathfrak{a})$ and $(\mathfrak{a}')$ are *mutual* commutators. Thus we are enabled to replace the equality (1.32) by *Wedderburn's theorem:**

$$\mathfrak{A} = (\mathfrak{b}')_t. \tag{1.33}$$

* This shortcut to Wedderburn's theorem was pointed out to me by R. Brauer.

THEOREM (1.3-B). *The relationship of a simple matrix algebra $\mathfrak{A}$ and its commutator algebra $\mathfrak{B}$ is mutual: $\mathfrak{A}$ is the full commutator algebra of $\mathfrak{B}$. $\mathfrak{B}$ is expressed in terms of a division algebra $\mathfrak{d}$ of order d as $t\cdot(\mathfrak{d})$, $\mathfrak{A}$ as $(\mathfrak{d}')_t$. Besides $h = tg$ we have $g = dt$, hence $h = dt^2$.*

From this follow two important consequences:

THEOREM (1.3-C). (Burnside.) *An irreducible $\mathfrak{A}$ of degree g whose only commutators are multiples αE of the unit matrix E (case $d = 1$) contains g^2 independent matrices (and is therefore irreducible in any field K over k; "absolute irreducibility").*

THEOREM (1.3-D). (*Criterion for irreducibility preserved.*) *The $\mathfrak{A}$ irreducible in k stays irreducible in a field K over k if its commutator algebra in K (as well as in k) is a division algebra.*

Indeed, our equation

$$\mathfrak{A} = (\mathfrak{d}')_t$$

at once leads to

$$\mathfrak{A}_K = (\mathfrak{d}'_K)_t$$

for the extensions to K. Under the assumption that $\mathfrak{d}_K$ and hence $\mathfrak{d}'_K$ is a division algebra, its regular representation $(\mathfrak{d}'_K)$ is irreducible in K and then so is $(\mathfrak{d}'_K)_t$.—The necessity of our criterion which has thus been shown to be sufficient is warranted by Schur's lemma.

The full reciprocity between algebra and commutator algebra is not reached before we pass from the irreducible representation $\mathfrak{A}$ of our simple algebra $\mathfrak{a}$ to a multiple $s\mathfrak{A}$. For this algebra $s\cdot(\mathfrak{d}')_t$ we readily find $t\cdot(\mathfrak{d})_s$ as its commutator algebra. The structure of the generic elements of our two algebras is indicated by the schemes

$$\tag{1.34} \begin{array}{|c|c|c|} \hline \begin{matrix} A_{11} & \cdots & A_{1t} \\ \cdots & \cdots & \cdots \\ A_{t1} & \cdots & A_{tt} \end{matrix} & 0 & \\ \hline 0 & \begin{matrix} A_{11} & \cdots & A_{1t} \\ \cdots & \cdots & \cdots \\ A_{t1} & \cdots & A_{tt} \end{matrix} & \\ \hline & & \\ \end{array} \qquad \begin{array}{|c|c|c} \hline \begin{matrix} B_{11} & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & B_{11} \end{matrix} & \begin{matrix} B_{12} & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & B_{12} \end{matrix} & \\ \hline \begin{matrix} B_{21} & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & B_{21} \end{matrix} & \begin{matrix} B_{22} & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & B_{22} \end{matrix} & \\ \hline & & \\ \end{array}$$

where all A_{ik} vary independently in $(\mathfrak{d}')$, all $B_{\alpha\beta}$ in $(\mathfrak{d})$; $i, k = 1, \cdots, t$; $\alpha, \beta = 1, \cdots, s$.

THEOREM (1.3-E). *A representation $\mathfrak{A}$ of a simple algebra has as its commutator a matrix algebra $\mathfrak{B}$ of the same type. The relationship is mutual: $\mathfrak{A}$ is the commutator algebra of $\mathfrak{B}$. More exactly, the structure is described by*

$$\mathfrak{A} = s\cdot(\mathfrak{d}')_t, \qquad \mathfrak{B} = t\cdot(\mathfrak{d})_s$$

where $\mathfrak{d}$ is an (abstract) division algebra of order d. The degree of $\mathfrak{A}$ and $\mathfrak{B}$ equals $d \cdot st$, order of $\mathfrak{A} = d \cdot t^2$, order of $\mathfrak{B} = d \cdot s^2$.

[The appendix 7 treats the automorphisms of algebras $\mathfrak{A}$ of the type here considered. Though we have no need for the facts there expounded, they follow so easily and naturally from our considerations that I could not resist the temptation of completing my account by their statement and proof.]

(1.4) Our next concern is a natural generalization of matrix algebras: the elements a may be n-uples

$$a = (A_1, A_2, \cdots, A_n)$$

of matrices in k, each component A_i being a matrix of prescribed degree g_i. Such elements may be added and multiplied among each other and multiplied by numbers in k by performing these operations on the several components separately. We want to study algebras $\mathfrak{a}$ in k consisting of such elements a. Each component like $A_1 = A_1(a)$ defines a representation $\mathfrak{A}_1$ of $\mathfrak{a}$: $a \rightarrow A_1$. The second part of Schur's lemma states that every matrix B in k satisfying the relation

$$A_1(a)B = BA_2(a)$$

identically in a must be zero provided the two component representations $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are irreducible and inequivalent. We prove:

THEOREM (1.4-A). *If the component representations of an n-uple matrix algebra $\mathfrak{a}$ are irreducible and inequivalent, then the n components A_i are independent of each other. (The regular representation of $\mathfrak{a}$, and hence every representation, is decomposable into irreducible parts each equivalent to one of the component representations.)*

The asserted "independence" may be formulated in different manners; the simplest formulation is perhaps as follows: if

$$a = (A_1, A_2, \cdots, A_n)$$

is contained in $\mathfrak{a}$, then the same holds for

$$\begin{aligned} a_1 &= (A_1, 0, \cdots, 0), \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ a_n &= (0, 0, \cdots, A_n). \end{aligned} \tag{1.41}$$

Or: with a varying over $\mathfrak{a}$, each component $A_i(a)$ varies *independently* over its whole range $\mathfrak{A}_i$; or: $\mathfrak{a}$ is the direct sum of the algebras $\mathfrak{A}_i$.

The proof follows exactly the lines laid out in the proof of Theorem (1.2-B). In an irreducible invariant subspace ϱ_1 of ϱ we picked out an element $a^0 \neq 0$. At least one of its n components A_i^0, let us say A_1^0, is $\neq 0$. We then chose a vector $\mathfrak{e}$ such that $A_1^0\, \mathfrak{e} \neq 0$, and concluded that ϱ_1 is similar to the first component space, i.e. the representation space of $\mathfrak{A}_1$ (or that the representation induced by the regular one in ϱ_1 is equivalent to $\mathfrak{A}_1$). We now add this little remark: For no element a in ϱ_1 can the second component A_2 be $\neq 0$. For then, starting with such an a instead of a^0 we should find that $\mathfrak{r}_1$ is similar to the second component space, which is impossible because of the inequivalence of $\mathfrak{A}_1$ and $\mathfrak{A}_2$. After the decomposition of $\mathfrak{r}$ into irreducible invariant subspaces $\mathfrak{r}_1, \mathfrak{r}_2, \cdots$ we unite those that are similar to the first component space, those similar to the second component space, and so on, and we thus arrive at the desired decomposition into independent components of form (1.41).

We finally consider a k-algebra $\mathfrak{a}$ of matrices in k which is decomposable into irreducible parts. Writing the equivalent ones among them alike, the generic element a breaks up into "blocks" of the kind:

$$\boxed{\begin{array}{ccc} A_i(a) & & \\ & \ddots & \\ & & A_i(a) \end{array}} \qquad (i = 1, \cdots v),$$

where

$$\mathfrak{A}_i : a \rightarrow A_i(a)$$

are irreducible and mutually inequivalent representations. The second part of Schur's lemma shows that each commutator breaks up into blocks of the same size. Together with our proposition concerning the independence of the several blocks in a, this leads to the culminating result[3] of our whole investigation:

THEOREM (1.4-B). *If a k-algebra $\mathfrak{A}$ of matrices in k is decomposable into irreducible parts, so is its commutator algebra $\mathfrak{B}$. $\mathfrak{A}$ is conversely the commutator algebra of $\mathfrak{B}$. Their structure is described by formulas*

$$\mathfrak{A} = \sum_{i=1}^{v} s_i(\mathfrak{d}_i')_{t_i}, \qquad \mathfrak{B} = \sum_{i=1}^{v} t_i(\mathfrak{d}_i)_{s_i}$$

where $\mathfrak{d}_i$, $\mathfrak{d}_i'$ are inverse (abstract) division algebras.

2. The Associated Linear Set and Algebra of a Riemann Matrix

(2.1) Two fields play a decisive part for Riemann matrices: the field k of *rational numbers* and that K of *real numbers.* One may replace k by any "real" field in the sense of the Artin-Schreier theory,[4] and K by a really closed real field over k; a real field k is of characteristic 0. No peculiar traits beyond that shall be made use of in our discussions, but it is pleasant to be able to refer to numbers in k and K respectively as "rational" and "real" numbers.

Let C be a symmetric or skew-symmetric non-singular rational matrix of

[3] Attributed to Rabinowitsch by v. d. Waerden, *Gruppen von linearen Transformationen*, Berlin, 1935, p. 53.

[4] *Abhandlungen Math. Sem. Hamburg,* vol. 5 (1926), pp. 85–99.

degree g, and $S = \| s_{ij} \|$ a symmetric real and positive-definite matrix of the same degree, i.e. one whose corresponding quadratic form

$$\sum_{i,j=1}^{g} s_{ij} x_i x_j$$

of the g real variables x_i is positive-definite. Then

$$R = C^{-1} S \tag{2.11}$$

is called a (*generalized*) *Riemann matrix*. The two cases $C' = \pm C$ are distinguished by the attribute *even* or *odd*. If the rational matrix A commutes with R, the Riemann matrix R is said to allow the *complex multiplication* A (it would probably be better to substitute the word "matric" for complex). About the significance of this concept for Riemann surfaces and their integrals, the necessary information is to be found in my note referred to above; we are concerned with the natural generalization of the problem of complex multiplication for elliptic functions from the genus 1 to arbitrary genus.

By a transformation U with rational coefficients one may introduce a new "rational" coördinate system in the underlying vector space. R is then changed into the equivalent $U^{-1}R\,U$, whereas C and S are to be transformed according to:

$$C \rightarrow U'\,C\,U\,, \qquad S \rightarrow U'\,S\,U\,.$$

The relation (2.11) or

$$CR = S \tag{2.12}$$

as well as the symmetries

$$C' = \pm C\,, \qquad S' = S \tag{2.13}$$

are then preserved. Later on we shall have occasion to use other "real" coördinate systems besides the rational ones. The positive-definite character of S has the consequence that (in an arbitrary real coördinate system) if we cut S:

$$S = \left\| \begin{matrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{matrix} \right\|$$

then not only S but the principal minors S_{11}, S_{22} as well are non-singular (and positive-definite).

(2.2) The first step one can take is to substitute for R the *smallest linear k-set Λ of matrices in k whose extension Λ_K to K contains R.* I call Λ the *associated linear set*. It provides the most complete reagent for the rational properties of R; for it exhibits them all while automatically extinguishing the transcendental features of R which the algebraist is so anxious to forget about. Two Riemann matrices whose associated linear sets are (rationally) equivalent may therefore be named *kindred* matrices. This closest rational kinship by no means implies the rational equivalence of the Riemann matrices themselves. The existence of a common cross-cut Λ of all linear k-sets of matrices in k, whose extension to K contains R, is established by the following considerations.

Let $L_1, \cdots, L_l$ and $M_1, \cdots, M_m$ be the bases of two such linear k-sets Λ and $\mathbf{M}$:

$$R = x_1^0 L_1 + \cdots + x_l^0 L_l = y_1^0 M_1 + \cdots + y_m^0 M_m$$

(x_i^0, y_k^0 real numbers). The solutions $(x_i; y_k)$ of the linear equations

$$x_1 L_1 + \cdots + x_l L_l = y_1 M_1 + \cdots + y_m M_m$$

with rational coefficients have a base consisting of *rational* solutions. When we express the particular solution $(x_i^0; y_k^0)$ as a linear combination of them, we express R as a linear combination of matrices common to Λ and $\mathbf{M}$.

Some obvious properties of the associated set Λ of base $L_1, \cdots, L_l$ are readily ascertained. The symmetry of (2.12) together with $C' = \pm C$ yields

$$R' C = \pm C R . \tag{2.21}$$

From every matrix L of Λ we form L_* by

$$L_*' = C L C^{-1} . \tag{2.22}$$

The extension to K of the linear set Λ_* thus obtained, involves R according to (2.21); hence $\Lambda \prec \Lambda_*$ and then $\Lambda = \Lambda_*$ because the order of Λ_* equals that of Λ; or the linear process $L \longrightarrow L_*$ carries each L of Λ into an L_* of Λ again. (2.22) may be written in both forms:

$$L_*'C = CL \quad \text{or} \quad CL_* = L'C \tag{2.23}$$

owing to $C' = \pm C$. Hence the same operation $L \rightarrow L_*$ carries L_* back into L and is therefore an *involution*. A rational commutator A of R is at the same time a commutator of Λ. Indeed, the solutions x_i of the rational linear equations $AL = LA$ for the generic element L of Λ_K:

$$L = x_1L_1 + \cdots + x_lL_l$$

have a rational base. We thus determine a linear subset within Λ whose ele ments L satisfy $AL = LA$ and whose extension to K includes R. The minimum property of Λ requires the subset to exhaust Λ. Adding a remark of similarly obvious nature, we sum up:

Theorem (2.2-A). *All linear k-sets of matrices in k whose extension to K involves R, have a common cross-cut of the same property,* $\Lambda = \{L\}$, *the associated linear set.* Λ *allows a linear involution* $L \rightarrow L_*$ *as defined by* (2.22). *The rational commutators of R and* Λ *coincide. Any rational reduction of R goes hand-in-hand with a parallel reduction of* Λ *and vice versa.*

The first non-trivial and encouraging fact about Riemann matrices is Poincaré's theorem of reduction:

Theorem (2.2-B). *The associated set* Λ *of a Riemann matrix* R *is decomposable into irreducible parts.*

Proof: With respect to a given reduction of $\Lambda = \{L\}$:

$$L = \begin{Vmatrix} L_{11} & 0 \\ L_{21} & L_{22} \end{Vmatrix}, \qquad R = \begin{Vmatrix} R_{11} & 0 \\ R_{21} & R_{22} \end{Vmatrix}$$

we write

$$C = \begin{Vmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{Vmatrix}, \qquad S = \begin{Vmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{Vmatrix}$$

$C_{22}\, R_{22} = S_{22}$ proves C_{22} to be non-singular. We infer from the equation $L'_*C = CL$ for

$$L'_* = \begin{Vmatrix} L^*_{11} & L^*_{12} \\ 0 & L^*_{22} \end{Vmatrix}, \qquad L = \begin{Vmatrix} L_{11} & 0 \\ L_{21} & L_{22} \end{Vmatrix}$$

the two relations

$$L^*_{22}C_{22} = C_{22}L_{22}\,,$$

$$L^*_{22}C_{21} = C_{21}L_{11} + C_{22}L_{21}\,.$$

One substitutes $L^*_{22} = C_{22}L_{22}C^{-1}_{22}$ from the first into the second equation, and gets

$$L_{22}C^{-1}_{22}C_{21} - C^{-1}_{22}C_{21}L_{11} = L_{21}\,.$$

This shows that the rational transformation

$$\begin{Vmatrix} E & 0 \\ B & E \end{Vmatrix}, \qquad B = C^{-1}_{22}C_{21}$$

effects the desired decomposition:

$$\begin{Vmatrix} E & 0 \\ B & E \end{Vmatrix} \cdot \begin{Vmatrix} L_{11} & 0 \\ L_{21} & L_{22} \end{Vmatrix} = \begin{Vmatrix} L_{11} & 0 \\ 0 & L_{22} \end{Vmatrix} \cdot \begin{Vmatrix} E & 0 \\ B & E \end{Vmatrix}.$$

After this has been accomplished:

$$L = \begin{Vmatrix} L_1 & 0 \\ 0 & L_2 \end{Vmatrix}, \qquad R = \begin{Vmatrix} R_1 & 0 \\ 0 & R_2 \end{Vmatrix},$$

and the relations

$$C_{11}R_1 = S_{11}, \qquad C_{22}R_2 = S_{22}$$

show that the parts R_1, R_2 are Riemann matrices.

(2.3) There is no machinery ready for handling linear matrix sets. However, when we remember that a matrix A commuting with two matrices L_1 and L_2

also commutes with L_1L_2, we are led to replace Λ by its algebraic closure $\mathfrak{L}$ in k. It arises when we form products of any number of elements of Λ and their linear combinations. $\mathfrak{L}$ is called *the associated algebra of* R, and two Riemann matrices are *associated* when they possess the same or equivalent associated algebras. This "association" is much weaker than the "kinship" before mentioned; many finer rational traits of R are effaced by substituting for Λ its embedding algebra $\mathfrak{L}$—the smallest k-algebra of k-matrices whose extension to K includes R. We thus take refuge in the mathematician's usual makeshift: if one can't solve a problem, one dilutes it so that one can. We have one strong excuse, however, in our case: we retain enough for the treatment of the problem of "matric multiplication." It is evident that the involutorial operation $L \rightarrow L_*$ defined by (2.22) takes place within $\mathfrak{L}$ as well as in Λ. Considered as an operation in the abstract algebra $\mathfrak{l}$ it is an involutorial anti-automorphism satisfying the rules

$$(p+q)_* = p_* + q_*, \qquad (\alpha p)_* = \alpha p_*, \qquad (pq)_* = q_*p_*$$

$$(p,\, q \text{ elements in } \mathfrak{l},\ \alpha \text{ a number in } k).$$

An algebra allowing an anti-automorphic involution $p \rightarrow p_*$ may be called *involutorial*. The *even* and *odd* elements are those satisfying the equations $p_* = p$, $p_* = -p$ respectively. Each element is the sum of an even and an odd element:

$$p = \tfrac{1}{2}(p + p_*) + \tfrac{1}{2}(p - p_*).$$

R is an even or odd element in the closure $\mathfrak{L}_K$ according as R is an even or odd Riemann matrix.

THEOREM (2.3). *The associated algebra* $\mathfrak{L}$ *of a Riemann matrix* R *is an involutorial algebra and decomposable into irreducible parts, each of which is associated with its own (rationally irreducible) Riemann matrix. The rational commutator algebra* $\mathfrak{A}$ *of* $\mathfrak{L}$ *coincides with that of* R. *Vice versa* $\mathfrak{L}$ *is the commutator algebra of* $\mathfrak{A}$.

The last remark, an immediate consequence of Theorem (1.4-B), affords a new definition of the associated algebra from which its properties could equally easily have been derived, and it shows that $\mathfrak{L}$ and $\mathfrak{A}$ both encompass exactly the same amount of information about the rational nature of R. Since

$$AL = LA \qquad \text{implies} \qquad L'A' = A'L',$$

$\mathfrak{A}$ as well as $\mathfrak{L}$ is involutorial, the involution in $\mathfrak{A}$: $A \rightarrow A^*$ being defined by the same equation (2.22):

$$A'_* = CAC^{-1}.$$

Our analysis of the structure of a fully decomposable matrix algebra $\mathfrak{L}$, by warranting the inequivalent irreducible parts to be independent variables, reduces the problem without any loss to the case of a rationally irreducible R and $\mathfrak{L}$. Thus for the rest of the paper we assume R as a *pure*, i.e. irreducible, Riemann matrix. *Our chief problem is to ascertain the necessary and sufficient conditions that a given algebra* $\mathfrak{L}$ *is a Riemann algebra, namely an algebra associated with some pure Riemann matrix* R.

3. Splitting Fields and Factor Sets, both Absolute and Relative

After the easy advance through open territory, the battle now starts in earnest. We had better put in place, therefore, our big guns: splitting field and factor set.

(3.1) First, some preliminary remarks about algebraic extensions of the reference field k (of characteristic 0).

An irreducible equation $f(x) = 0$ of degree n with coefficients in k determines a field $k(\vartheta)$ of degree n; $f(\vartheta) = 0$. Each number η in $k(\vartheta)$ is of the form

$$\eta = e_0 + e_1\vartheta + \cdots + e_{n-1}\vartheta^{n-1} \qquad (e_i \text{ in } k). \tag{3.11}$$

In some field over k, $f(x)$ breaks up into n different linear factors:

$$f(x) = \prod_{\alpha=1}^{n} (x - \vartheta_\alpha).$$

We have the n *conjugations* $\vartheta \longrightarrow \vartheta_\alpha$ sending η, (3.11) over into

$$\eta_\alpha = e_0 + e_1\vartheta_\alpha + \cdots + e_{n-1}\vartheta_\alpha^{n-1}. \tag{3.12}$$

The n fields $k(\vartheta_\alpha)$ are, as it were, copies of the model $k(\vartheta)$ which no one can algebraically tell apart; each field does exactly the same as the other, like show girls in a parade. When looked upon as a linear transformation between variables e_i and η_α the Vandermonde transformation (3.12), V_n, is non-singular.

Two pairs of indices (α, β) and (α', β') are *conjugate* when a permutation of the Galois group carries ϑ_α, ϑ_β into $\vartheta_{\alpha'}$, $\vartheta_{\beta'}$; or when each polynomial $F(x, y)$ in k vanishing for $x = \vartheta_\alpha$, $y = \vartheta_\beta$ also vanishes for $\vartheta_{\alpha'}$, $\vartheta_{\beta'}$. A number

$$\eta_{\alpha\beta} = G(\vartheta_\alpha, \vartheta_\beta)$$

in $k(\vartheta_\alpha, \vartheta_\beta)$ then has a definite conjugate $\eta_{\alpha'\beta'} = G(\vartheta_{\alpha'}, \vartheta_{\beta'})$ not affected by what is arbitrary in the choice of the polynomial $G(x, y)$ in k. A double set

$$\eta_{\alpha\beta} \qquad (\alpha, \beta = 1, \cdots, n)$$

is called a *conjugate set* provided each $\eta_{\alpha\beta}$ lies in $k(\vartheta_\alpha, \vartheta_\beta)$, and $\eta_{\alpha\beta}$ and $\eta_{\alpha'\beta'}$ are conjugate whenever the two pairs (α, β) and (α', β') are conjugate. It is readily seen that such a conjugate set may be represented by a formula

$$\eta_{\alpha\beta} = \sum_{i,j=0}^{n-1} e_{ij}\vartheta_\alpha^i\vartheta_\beta^j \qquad (e_{ij} \text{ in } k). \tag{3.13}$$

Nevertheless our original and less formal definition is preferable in view of its easier management. Analogous definitions apply to triple sets, and so on.

A subfield κ of $k(\vartheta)$ over k of degree v determines a partition of the indices α into v classes Γ of m "*coördinated*" indices each: α and β are called coördinated if $\eta_\alpha = \eta_\beta$ for all numbers η in κ. Any given coördination of the n indices into classes can thus be generated provided coördination is not destroyed by conjugation: whenever α, β are coördinated and the pair (α', β') is conjugate to (α, β), we suppose that then α', β' are coördinated also.

The term "conjugate double set" $\eta_{\alpha\beta}$ (or triple set, and so on) keeps a definite meaning if we assume $\eta_{\alpha\beta}$ to be defined merely for coördinated subscripts α, β; we then speak of a *conjugate set over* κ. Instead of (3.13) it is more convenient to use a representation

$$\eta_{\alpha\beta} = \sum_{i,j=0}^{m-1} e_\Gamma^{ij} \vartheta_\alpha^i \vartheta_\beta^j \tag{3.14}$$

where e^{ij} is a number in κ and e_Γ^{ij} denotes the conjugate $e_\alpha^{ij} = e_\beta^{ij} = \cdots$ for the class $\Gamma = \alpha, \beta, \cdots$ of coördinated indices.

(3.2) Let $\mathfrak{l}$ be a *simple algebra* in k of order h and $\mathfrak{L}$: $l \rightarrow L$ its irreducible faithful representation of degree g by which $\mathfrak{l}$ was defined; $h = tg$. I. Schur constructed the *splitting field* in the following manner.[5]

We take a rational commutator A of $\mathfrak{L}$. Since every root ϑ of the characteristic polynomial $\varphi(z)$ of A satisfies the equation $| A - \vartheta E | = 0$ the relation $| \psi(A) | = 0$ holds for every factor $\psi(z)$ of $\varphi(z)$; we suppose that $\psi(z)$ lies in k and is irreducible in k. But then as the commutator algebra $\mathfrak{A}$ of the irreducible $\mathfrak{L}$ is a division algebra, not only the determinant but the matrix $\psi(A)$ itself must vanish. In the g-dimensional vector space $\mathbf{P}$ where A represents a linear substitution, we choose an arbitrary vector $\mathfrak{e} \neq 0$ (with rational coefficients) and form successively

$$\mathfrak{e}_0 = \mathfrak{e}, \qquad \mathfrak{e}_1 = A\mathfrak{e}_0, \qquad \mathfrak{e}_2 = A\mathfrak{e}_1, \cdots.$$

If ψ is of degree n, one derives from the equation $\psi(A) = 0$ and the irreducibility of ψ the fact that the vectors $\mathfrak{e}_0, \mathfrak{e}_1, \cdots, \mathfrak{e}_{n-1}$ span an n-dimensional subspace $\mathbf{P}_1$ of $\mathbf{P}$ which is invariant with respect to A and in which $\psi(z)$ is the characteristic polynomial of A. Starting with a vector $\mathfrak{e}_0'$ not contained in $\mathbf{P}_1$, the same procedure furnishes a second independent subspace $\mathbf{P}_2$ in which the same is true; and so forth. Therefore one must have

$$\varphi(z) = (\psi(z))^f, \qquad g = fn.$$

If

$$\psi(z) = \prod_{\alpha=1}^{n} (z - \vartheta_\alpha)$$

the matrix of the transformation A of $\mathbf{P}_1$, when expressed in the coördinate system $\mathfrak{e}_0, \mathfrak{e}_1, \cdots, \mathfrak{e}_{n-1}$, is changed by the Vandermonde transformation (3.12), V_n, into the diagonal matrix

$$\begin{Vmatrix} \vartheta_1 & & \\ & \ddots & \\ & & \vartheta_n \end{Vmatrix}.$$

[5] *Transactions Amer. Math. Soc.* (2) **15** (1909), p. 159.

The result is this: in an "irrational" coördinate system changing into a rational one by the Vandermonde transformation $V_n \times E_f$, the matrix A appears as the diagonal matrix of the roots

$$\vartheta_1, \cdots, \vartheta_1, \vartheta_2, \cdots, \vartheta_2, \cdots, \vartheta_n, \cdots, \vartheta_n \qquad \text{(each root } f \text{ times).}$$

Since the ϑ_α are all distinct, the generic element L of $\mathfrak{L}$, since it satisfies the equation $AL = LA$, splits up in the same coördinate system in the following way:

$$\left\| \begin{matrix} L_1 & & \\ & \ddots & \\ & & L_n \end{matrix} \right\| \sim L,$$

where $L_\alpha = L(\vartheta_\alpha)$ are conjugate matrices of degree f in the conjugate fields $k(\vartheta_\alpha)$. ($\sim$ stands for: "changes into . . . by the Vandermonde transformation $V_n \times E_f$.") The L_α form the algebra $\mathfrak{L}_\alpha$; the algebra of the $L(\vartheta)$ may be designated by $\mathfrak{L}(\vartheta)$ if ϑ is any one of the roots ϑ_α, no matter which. $\mathfrak{L}(\vartheta)$ is irreducible in $k(\vartheta)$ because a reduction in $k(\vartheta)$ would result in a rational reduction of $\mathfrak{L}$.

The number field $k(\vartheta)$ is isomorphic to the field $k(a)$ consisting of the polynomials of $a = A$ with coefficients in k. If we have an element $b = B$ in the commutator algebra $\mathfrak{A}$ commuting with a, the splitting can be pushed forward, for then, in the irrational coördinate system just introduced, B decomposes like L into conjugate matrices B_α; B_α is a commutator of $\mathfrak{L}_\alpha$. In applying the above consideration on B_α rather than on A and in the field $k(\vartheta_\alpha)$ instead of k, we bring B_α into diagonal form and obtain a corresponding splitting of L_α. Only then the splitting made no headway when b belongs to the field $k(a)$. In this manner one finally arrives by successive adjunctions of elements a of $\mathfrak{A}$ commutable among each other, at a *maximal* a which has the property that each element b of $\mathfrak{A}$ commutable with a lies in $k(a)$. Our notations shall now refer to such a maximal a; the number field $k(\vartheta)$ isomorphic to $k(a)$ is then called a *splitting field*. Under these circumstances the multiples of the unit matrix are the only matrices commuting with all members $L(\vartheta)$ of the $k(\vartheta)$-irreducible algebra $\mathfrak{L}(\vartheta)$; hence, according to Burnside's theorem, $\mathfrak{L}(\vartheta)$ contains f^2 linearly independent matrices and is *absolutely irreducible*.

[In a more general way the field $k(\eta)$ of degree r is called a splitting field for $\mathfrak{l}$ if $\mathfrak{l}$ allows of an absolutely irreducible representation in $k(\eta)$. One readily concludes from the fact that each representation of $\mathfrak{l}$ is a multiple of the irreducible one $\mathfrak{L}$, that the degree r is a multiple of n. We shall here avail ourselves only of the splitting fields of minimum degree n derived from the commutator algebra.]

(3.3) Two of the conjugate representations $\mathfrak{L}_\alpha$, $\mathfrak{L}_\beta$ may be either equivalent or not. In the second case the equation

$$BL_\beta = L_\alpha B$$

when required to hold for all elements L has by the Schur lemma the only solution $B = 0$, in a field K involving all $k(\vartheta_\alpha)$. In the first case there exists a non-singular solution B; each solution is a multiple of B and hence either 0 or non-singular. In particular, the equation obviously has a solution $A_{\alpha\beta} \neq 0$ lying in $k(\vartheta_\alpha, \vartheta_\beta)$, if it has a non-vanishing solution at all; $| A_{\alpha\beta} | \neq 0$. We say that the two conjugations $\vartheta \rightarrow \vartheta_\alpha$ and $\vartheta \rightarrow \vartheta_\beta$ are coördinated provided $\mathfrak{L}_\alpha$ and $\mathfrak{L}_\beta$ are equivalent. Since

$$A_{\alpha\beta}L_\beta = L_\alpha A_{\alpha\beta} \tag{3.31}$$

implies

$$A_{\alpha'\beta'}L_{\beta'} = L_{\alpha'}A_{\alpha'\beta'},$$

if (α', β') is conjugate to (α, β) this coördination has the property mentioned under (3.1), and is hence being generated by a certain subfield κ of degree v, the *central field*; $n = v \cdot m$. The quotient m is called the *Schur index* of $\mathfrak{L}$. We are able to determine the non-singular $A_{\alpha\beta}$ such that $A_{\alpha\alpha} = E_f$ and such that they form a conjugate double set over κ. In the future, subscripts α or $\alpha\beta$ or $\alpha\beta\gamma$ are always meant to indicate that we are concerned with a conjugate set over κ.

On passing into a field K involving all the conjugate fields $k(\vartheta_\alpha)$ one sees from Burnside's theorem and its supplement (1.4-A) that the order h of $\mathfrak{L}$ equals $v \cdot f^2$. From this follows by means of

$$h = tg = tfn = tfvm$$

that

$$f = tm. \tag{3.32}$$

The arbitrariness in choosing the $A_{\alpha\beta}$ consists in the possibility of replacing $A_{\alpha\beta}$ by $e_{\alpha\beta}A_{\alpha\beta}$; $e_{\alpha\alpha} = 1$, $e_{\alpha\beta} \neq 0$.

The equivalences $\mathfrak{L}_\alpha \sim \mathfrak{L}_\beta$, $\mathfrak{L}_\beta \sim \mathfrak{L}_\gamma$:

$$A_{\alpha\beta}L_\beta = L_\alpha A_{\alpha\beta}, \qquad A_{\beta\gamma}L_\gamma = L_\beta A_{\beta\gamma}$$

in the following way result in the equivalence $\mathfrak{L}_\alpha \sim \mathfrak{L}_\gamma$:

$$A_{\alpha\beta}A_{\beta\gamma} \cdot L_\gamma = L_\alpha \cdot A_{\alpha\beta}A_{\beta\gamma}.$$

Hence a relation

$$A_{\alpha\beta}A_{\beta\gamma} = c_{\alpha\beta\gamma}A_{\alpha\gamma} \tag{3.33}$$

must hold. The conjugate numbers $c_{\alpha\beta\gamma} \neq 0$ form the *factor set*. From (3.33) and $A_{\alpha\alpha} = E$ follows at once

$$\begin{cases} c_{\alpha\alpha\beta} = 1, \qquad c_{\alpha\beta\beta} = 1; \\ c_{\alpha\beta\gamma} \cdot c_{\alpha\gamma\delta} = c_{\alpha\beta\delta} \cdot c_{\beta\gamma\delta}. \end{cases} \tag{3.34}$$

If one replaces $A_{\alpha\beta}$ by $e_{\alpha\beta}A_{\alpha\beta}$ the factor set c is changed into the "equivalent" c^*:

$$c^*_{\alpha\beta\gamma} = \frac{e_{\alpha\beta}e_{\beta\gamma}}{e_{\alpha\gamma}} \cdot c_{\alpha\beta\gamma}.$$

The splitting field once chosen, the factor set is uniquely determined by $\mathfrak{l}$ in the sense of equivalence.

(3.4) Conversely $\mathfrak{L}$ *is uniquely determined by its factor set in the sense of equivalence.* The proof obviously must depend on ascertaining the following two facts: 1) A matrix M,

$$(3.41) \qquad \left\| \begin{matrix} M_1 & & \\ & \ddots & \\ & & M_n \end{matrix} \right\| \sim M,$$

whose parts M_α form a conjugate set of matrices satisfying the equations (3.31):

$$(3.42) \qquad A_{\alpha\beta} M_\beta = M_\alpha A_{\alpha\beta}$$

necessarily lies in $\mathfrak{L}$. 2) If a second system $A^*_{\alpha\beta}$ satisfies the same equations (3.33) as $A_{\alpha\beta} (A^*_{\alpha\alpha} = E)$, then

$$(3.43) \qquad A^*_{\alpha\beta} = T_\alpha^{-1} A_{\alpha\beta} T_\beta$$

where T_α are conjugate non-singular matrices.

Proof of 1). M, if defined according to (3.41) by means of arbitrary matrices M_α in K which fulfill the equations (3.42), contains just the right number $v \cdot f^2$ of parameters and is hence contained in the closure $\mathfrak{L}_K$. If in addition, the M_α are conjugate matrices in $k(\vartheta_\alpha)$, the matrix M itself is rational and hence lies in $\mathfrak{L}$. [By the way, our proposition shows that the matrix L defined by $L_\alpha = \eta_\alpha E$ lies in $\mathfrak{L}$ provided η is any number of the central field; which proves that in the isomorphism $a \to \vartheta$ the central field corresponds to that subfield of $k(a)$ which consists of the centrum elements of $\mathfrak{A}$.]

Proof of 2).

$$T_\alpha = A^{*-1}_{\rho\alpha} A_{\rho\alpha}$$

satisfies the equation (3.43) for every fixed ρ (coördinated with $\alpha, \beta, \cdots$); the only trouble is that this is not a matrix lying in $k(\vartheta_\alpha)$! We therefore form

$$(3.44) \qquad T_\alpha = \sum_\rho \zeta_\rho A^{*-1}_{\rho\alpha} A_{\rho\alpha}$$

by means of an arbitrary number ζ of $k(\vartheta)$ and must try to take care that the determinant $| T_\alpha | \neq 0$. When we put (Vandermonde transformation!)

$$\zeta_\rho = z_0 + z_1 \vartheta_\rho + \cdots + z_{n-1} \vartheta_\rho^{n-1}$$

the determinant $| T_1 |$ is a polynomial of the variables $z_0, z_1, \cdots, z_{n-1}$ that does not vanish identically since $| T_1 | = 1$ for $\zeta_1 = 1, \zeta_\rho = 0 \ (\rho \neq 1)$. Consequently there exist also *values* z_i *in* k for which $| T_1 | \neq 0$; then the T_α are non-singular conjugate matrices. 2) in particular contains Speiser's theorem: if $A_{\alpha\beta} A_{\beta\gamma} = A_{\alpha\gamma}$, then there exist non-singular conjugate matrices T_α such that $A_{\alpha\beta} = T_\alpha^{-1} T_\beta$.

[The existential question is the following: Given a field $k(\vartheta)$ of degree $n = v \cdot m$ and a subfield $\kappa = k(\eta)$ of degree v; the conjugations $\vartheta \to \vartheta_\alpha$, $\vartheta \to \vartheta_\beta$

are called coördinated if $\eta_\alpha = \eta_\beta$. Furthermore, given a set of numbers $c_{\alpha\beta\gamma} \neq 0$ conjugate over κ and satisfying the relations (3.34): Does there exist a simple algebra for which $k(\vartheta)$, κ, $c_{\alpha\beta\gamma}$ play the part of splitting field, central field, and factor set, respectively? Brauer answers it affirmatively by giving an example;[6] the equations (3.33) have a solution $A_{\alpha\beta}$ *of degree m*. But what one obtains may correspond to the more general situation only cursorily mentioned above, that one failed to choose a splitting field of minimum degree. If one wishes to exclude this, one has to assume in addition that the given factor set is of *Schur index m*, i.e., that the equations (3.33) allow of no solution of lower degree than m.]

(3.5) We need a certain generalization of the theory of splitting fields which I contrast, by the word *"relative,"* to the *absolute* splitting fields heretofore studied. The splitting of $\mathfrak{L}$ into the $\mathfrak{L}_\alpha$ may have been accomplished again by an element a of the commutator algebra. We apply the old notations. However, we shall now assume only that the parts $\mathfrak{L}_\alpha$ are irreducible in a given field K including the n conjugate fields $k(\vartheta_\alpha)$. (For the application to Riemann matrices, K will be the "real" field.) That is to say, we rise merely to the level K rather than to "absolute" irreducibility. In following the above procedure we are to consider those elements Q of $\mathfrak{A}$ that commute with A. There occur the parallel decompositions

$$A \text{ in } \vartheta_\alpha E\,, \qquad Q \text{ in } Q_\alpha\,, \qquad L \text{ in } L_\alpha\,.$$

The extension of the linear set $\mathfrak{Q}_\alpha$ of all Q_α to $k(\vartheta_\alpha)$ may be called $\mathfrak{Q}^{(\alpha)}$. As $\mathfrak{L}_\alpha$ is irreducible in $k(\vartheta_\alpha)$, this $\mathfrak{Q}^{(\alpha)}$ is a division algebra of a certain order d in $k(\vartheta_\alpha)$, the abstract scheme of which may be called $\mathfrak{q}^{(\alpha)}$. The laws of composition in the several $\mathfrak{q}^{(\alpha)}$ are conjugate to each other in the fields $k(\vartheta_\alpha)$; they are copies of a model division algebra $\mathfrak{q}$ in $k(\vartheta)$. The element $q^{(\alpha)}$ of $\mathfrak{q}^{(\alpha)}$ is represented in $\mathfrak{Q}^{(\alpha)}$ by the matrix $Q^{(\alpha)} = (q^{(\alpha)}) \times E_f$ where $(q^{(\alpha)})$ denotes the regular representation of $q^{(\alpha)}$ in $\mathfrak{q}^{(\alpha)}$. The former notation is changed to the effect that now $d\cdot f$ is the degree of the matrices $Q^{(\alpha)}$, L_α. The order of $\mathfrak{L}_\alpha$ is $d\cdot f^2$ according to Theorem (1.3-B).

Since $\mathfrak{L}_\alpha$ is irreducible in K, $\mathfrak{q}^{(\alpha)}$ remains a division algebra when we close it in K: $\mathfrak{q}_K^{(\alpha)}$. The elements $q^{(\alpha)}$ of $\mathfrak{q}_K^{(\alpha)}$ shall be called *α-quantics*. The upper index (α) shall always indicate an α-quantic. The situation is now perfectly analogous to the previous one but for the fact that quantics take the place of scalars.

α and β are coördinated provided $\mathfrak{L}_\alpha$ and $\mathfrak{L}_\beta$ are equivalent in K. The coördination is effected by a subfield κ of $k(\vartheta)$, the central field of degree v. According to Theorem (1.4-A) the v non-coördinated parts $\mathfrak{L}_\alpha$ are entirely independent of each other in the closure $\mathfrak{L}_K$. The order of $\mathfrak{L}$ is therefore $h = v\cdot df^2$;

[6] *Math. Zeitschrift* vol. 28 (1928), pp. 677–696, in particular §6, p. 682.—The whole theory of factor sets is due to R. Brauer: *Sitzungsber. Berl. Akad.* (1926), pp. 410–416. Compare furthermore: R. Brauer, *Math. Zeitschrift*, vol. **30** (1929), pp. 79–107.

comparison with the degree $g = mvdf$ again leads to the relation $f = tm$. The equation

$$BL_\beta = L_\alpha B\,, \tag{3.51}$$

when required to hold for all L has only the solution $B = 0$ if α and β are not coördinated. If they are coördinated, however, it has a non-singular solution B, and every solution $Q^{(\alpha)}B = q^{(\alpha)}B$ arises from it by fore multiplication with an α-quantic—or by aft multiplication with a β-quantic:

$$q^{(\alpha)}B = Bq^{(\beta)}\,. \tag{3.52}$$

Any solution different from zero is therefore non-singular. B, by means of (3.52), establishes an isomorphism T: $q^{(\alpha)} \leftrightarrow q^{(\beta)}$ between the α- and the β-quantics. Let us stop for a moment to consider how this isomorphism is changed when one replaces B by $b^{(\alpha)}B(= Bb^{(\beta)})$ ($b^{(\alpha)}$, an α-quantic). The new isomorphism is defined by

$$q^{(\alpha)}b^{(\alpha)}B = b^{(\alpha)}Bq^{(\beta)}\,. \tag{3.53}$$

We form

$$b^{(\alpha)-1}\, q^{(\alpha)}\, b^{(\alpha)} = \bar{q}^{(\alpha)}\,. \tag{3.54}$$

Then (3.53) reads:

$$\bar{q}^{(\alpha)}B = Bq^{(\beta)}\,,$$

and consequently $\bar{q}^{(\alpha)} \to q^{(\beta)}$ is the old isomorphism T. The modification consists in letting T be preceded by the inner automorphism (3.54), $q^{(\alpha)} \to \bar{q}^{(\alpha)}$, of the α-quantics generated by $b^{(\alpha)}$ (or in having the inner automorphism $[b^{(\beta)}]$ of the β-quantics follow T). The inner automorphism generated by an element b is briefly denoted by $[b]$.

It is perhaps advisable to describe our "quantics" a little more carefully. Each quantic x is given as a set of d numbers $(x_1, \cdots, x_d)$ in K; the coefficients π in the multiplication law

$$xy = z\colon\ z_i = \sum_{k,l} \pi^{ikl} x_k y_l \qquad (i, k, l = 1, \cdots, d)$$

are numbers in $k(\vartheta)$. Transition to a new base is described by equations

$$x_i = \sum_k \tau^{ik} \bar{x}_k \qquad (|\tau^{ik}| \neq 0)$$

with coefficients τ^{ik} in $k(\vartheta)$; only such relations are to be studied as are invariant under arbitrary changes in base of this type. We manufacture n copies $\mathfrak{q}^{(\alpha)}$ of this model $\mathfrak{q}$ (α-quantics, $\alpha = 1, \cdots, n$) by replacing the π^{ikl} by their conjugates π_α^{ikl} in $k(\vartheta_\alpha)$. A change of base takes place simultaneously in all n copies, the coefficients τ^{ik} being replaced by the conjugates τ_α^{ik} in the α^{th} copy (think of the show girls again!). It has an invariantive meaning to say that an α-quantic $x^{(\alpha)} = (x_1^{(\alpha)}, \cdots, x_d^{(\alpha)})$ lies, let us say, in $k(\vartheta_\alpha, \vartheta_\beta)$: $x_i^{(\alpha)}$ in $k(\vartheta_\alpha, \vartheta_\beta)$; and it has an invariantive meaning to assert that a set $x^{(\alpha)}_{\alpha\beta}$ of quantics are conjugate (over κ). It has an invariantive meaning to state that a given isomorphism T between the α- and β-quantics:

$$x^{(\alpha)} \leftrightarrow x^{(\beta)}: \; \bar{x}_i^{(\beta)} = \sum_j \sigma_{ij} x_j^{(\alpha)}$$

lies in $k(\vartheta_\alpha, \vartheta_\beta)$: σ_{ij} in $k(\vartheta_\alpha, \vartheta_\beta)$; and that a set $T_{\alpha\beta}$ of such isomorphisms is conjugate over κ.

If α and β are coördinated, (3.51) has a solution $B = A_{\alpha\beta} \neq 0$ in $k(\vartheta_\alpha, \vartheta_\beta)$; it is non-singular. We take care that $A_{\alpha\alpha} = E$ and $A_{\alpha\beta}$ form, as their notation indicates, a conjugate set over κ. By means of the formula

$$q^{(\alpha)} A_{\alpha\beta} = A_{\alpha\beta} q^{(\beta)} \tag{3.55}$$

$A_{\alpha\beta}$ determines an isomorphism $T_{\alpha\beta}$: $q^{(\alpha)} \leftrightarrow q^{(\beta)}$ between the α- and the β-quantics; again, the $T_{\alpha\beta}$ are conjugate over κ. We must have an equation

$$A_{\alpha\beta} A_{\beta\gamma} = c^{(\alpha)}_{\alpha\beta\gamma} A_{\alpha\gamma} \; (= A_{\alpha\gamma} c^{(\gamma)}_{\alpha\beta\gamma}), \tag{3.56}$$

the c's being a triple set of conjugate quantics $\neq 0$. This equation proves that the succession of the two isomorphisms

$$T_{\alpha\beta}: q^{(\alpha)} \longrightarrow q^{(\beta)}, \qquad T_{\beta\gamma}: q^{(\beta)} \longrightarrow q^{(\gamma)}$$

results in an isomorphism between the α- and γ-quantics, equal to $T_{\alpha\gamma}$ preceded by the inner automorphism $[c^{(\alpha)}_{\alpha\beta\gamma}]$. When we remember our convention that subscripts α or $\alpha\beta$ or $\alpha\beta\gamma$ shall automatically indicate that the terms are conjugate over κ, and that an upper index (α) designates an α-quantic, we may finally describe *a quantic factor set* as follows:

Given a field $k(\vartheta)$ of degree n over k; a subfield κ of degree v, $n = v \cdot m$, determines the coördinating of the conjugations $\vartheta \longrightarrow \vartheta_\alpha$ into v classes; a field K encompasses all conjugate fields $k(\vartheta_\alpha)$.

Given a division algebra $\mathfrak{q}$ of "quantics" in K of the nature above described: the multiplication law has coefficients π in $k(\vartheta)$ and only base transformations with coefficients τ in $k(\vartheta)$ are allowed. We then have the n conjugate copies $\mathfrak{q}^{(\alpha)}$ of the model $\mathfrak{q}$: α-quantics.

A factor set consists: 1) *of a κ-conjugate set of isomorphisms $T_{\alpha\beta}$: $q^{(\alpha)} \leftrightarrow q^{(\beta)}$, and* 2) *a κ-conjugate set of quantics $\neq 0$:*

$$c^{(\alpha)}_{\alpha\beta\gamma} \leftrightarrow c^{(\gamma)}_{\alpha\beta\gamma} \tag{3.57}$$

such that the succession of $T_{\alpha\beta}$ and $T_{\beta\gamma}$ results in $T_{\alpha\gamma}$ preceded by the inner automorphism $[c^{(\alpha)}_{\alpha\beta\gamma}]$ (or succeeded by the inner automorphism $[c^{(\gamma)}_{\alpha\beta\gamma}]$). The following conditions prevail:

$$\begin{cases} c^{(\alpha)}_{\alpha\alpha\beta} = 1, \quad c^{(\beta)}_{\alpha\beta\beta} = 1, \\ c^{(\alpha)}_{\alpha\beta\gamma} \cdot c^{(\alpha)}_{\alpha\gamma\delta} \leftrightarrow c^{(\delta)}_{\alpha\beta\delta} \cdot c^{(\delta)}_{\beta\gamma\delta}. \end{cases} \tag{3.58}$$

In analogy to proposition 1) in (3.4), we have the

LEMMA (3.5): A matrix M in k breaking up into parts M_α will lie in $\mathfrak{L}$ provided M_α commutes with all the $Q^{(\alpha)}$ and the relations

$$A_{\alpha\beta}M_\beta = M_\alpha A_{\alpha\beta}$$

are satisfied for each pair of coördinated indices α, β.

The proof is the same as before: these conditions reduce the number of parameters in M to the right value $v \cdot df^2$.

[Ascent from our present level K to the absolute is accomplished by means of a "maximum" element q of $\mathfrak{q}$ lying in $k(\vartheta)$; it cracks each $\mathfrak{L}_\alpha$ into absolutely irreducible parts according to the numerically distinct roots of q.

Of particular interest is the special case that our quantics are commutative. Then we have

$$T_{\beta\gamma}T_{\alpha\beta} = T_{\alpha\gamma} ,$$

hence by Speiser's theorem: $T_{\alpha\beta} = T_\beta T_\alpha^{-1}$. This means: there exists a base for $\mathfrak{q}$ in terms of which the multiplication law has coefficients in κ. $\mathfrak{q}$ may then be described as a commutative field over κ that is not reduced by the extension of the reference field κ to K.]

4. Splitting Field of a Riemann Algebra

(4.1) Now let $\mathfrak{L}$ be again the irreducible algebra of matrices in k associated with a pure Riemann matrix $R = C^{-1}S$ and $\mathfrak{A}$ its commutator algebra. In $\mathfrak{L}$ and $\mathfrak{A}$ we have the anti-automorphic involutions $L \to L_*$, $A \to A_*$ generated by C.

LEMMA (4.1) (Rosati). *If A is an even element of the commutator algebra, its roots are real and C and S break up like $\mathfrak{L}$ into parts C_α, S_α according to the numerically distinct roots. The roots of an odd A are pure imaginary.*

For the proof of this lemma it is convenient to operate in the algebraically closed field $(K, \sqrt{-1})$ and to transform C and S in the manner

$$C \to \bar{U}'CU , \qquad S \to \bar{U}'SU \qquad (L \to U^{-1}LU)$$

by means of the transformation U carrying A into its diagonal form. The equation $CR = S$ is preserved and after the transformation, S is the coefficient matrix of a positive definite Hermitian form:

$$\bar{S}' = S , \qquad \bar{C}' = \pm C .$$

A_* is now defined by $\bar{A}_*' = CAC^{-1}$ and thus our even A satisfies the equation

$$\bar{A}'C = CA . \tag{4.11}$$

We broke A into parts $\vartheta_\alpha E$ where ϑ_α are the numerically distinct roots of A $(\alpha = 1, \cdots , n)$. The matrix C is accordingly checkered into squares $C_{\alpha\beta}$, and (4.11) reduces to

$$(\bar{\vartheta}_\alpha - \vartheta_\beta)C_{\alpha\beta} = 0 . \tag{4.12}$$

On account of $CR = S$:

$$C_{\alpha\beta}R_\beta = S_{\alpha\beta}\,,$$

$C_{\alpha\alpha}$ is non-singular and hence (4.12) requires:

$$\bar{\vartheta}_\alpha = \vartheta_\alpha\,, \qquad C_{\alpha\beta} = 0 \quad (\text{for } \alpha \neq \beta)\,.$$

Since the roots ϑ_α are real the corresponding Vandermonde transformation U is also real.

The case of an odd A is treated along the same lines.

(4.2) We now proceed in the same manner as in (3.2), with the difference, however, that only *even* elements a of $\mathfrak{A}$ shall be used for the purpose of splitting. As long as it is still possible to find even elements b commuting with a and not included in the field $k(a)$, one goes on adjoining them until one finds an even a such that every even b commuting with a lies in the field $k(a)$; by this a we determine our *splitting field* $k(\vartheta)$. Rosati's lemma tells us that all the conjugate ϑ_α are real, or that ϑ is a "totally real algebraic number" over k. Stopping here has the disadvantage that we do not get an "absolute" splitting field; the situation is rather that described in (3.5) with the real field K as the level reached. Indeed, the elements $q = Q$ of $\mathfrak{A}$ commuting with our maximal even a form a division algebra over $k(a)$ in which every element q satisfies a quadratic equation in $k(a)$. For if q commutes with a, so does q_*, and $q + q_*$ and qq_* are even and commute with a; they therefore lie in $k(a)$. The relation

$$q^2 - q(q + q_*) + qq_* = 0$$

is obvious. Now the only division algebras over a field $k(\vartheta)$ in which each element satisfies a quadratic equation in the reference field are of the following three types:[7]

I. the "*scalar*": elements q = numbers q_0 in the reference field $k(\vartheta)$;

II. the "*square root*": elements are of form $q_0 + q_1\iota$ where $\iota^2 = -\lambda$; q_0, q_1 vary in $k(\vartheta)$, $-\lambda$ lies, and is not square, in $k(\vartheta)$;

III. the "*quaternion*": elements are of form

$$q_0 + q_1\iota_1 + q_2\iota_2 + q_3\iota_3$$

where

$$\iota_1\iota_2 = -\iota_2\iota_1 = \iota_3\,, \qquad \iota_1^2 = -\lambda\,, \qquad \iota_2^2 = -\mu$$

and q_0, q_1, q_2, q_3 vary in the reference field while $-\lambda$ and $-\mu$ lie, and are no squares, in $k(\vartheta)$.

Thus one of these three types plays the rôle of our algebra $\mathfrak{q}$ of "quantics." The Rosati lemma, however, provides some more information. In the case of II and III the elements q represented by ι or ι_1, ι_2 satisfy an irreducible *pure*

[7] Cf. for example: L. E. Dickson, *Algebren und ihre Zahlentheorie*, Zürich (1927), pp. 43–45.

quadratic equation in $k(\vartheta)$, and hence $q + q_* = 0$, or q is odd. Therefore its roots must be pure imaginary, or λ in case II and λ, μ in case III are *totally positive* (all the conjugates λ_α; λ_α, μ_α respectively, are positive). For this reason we call the square root II and the quaternion III *"totally negative."* In consequence thereof, *each of the algebras* I, II, III *in all their n conjugate "copies"* $\mathfrak{q}^{(\alpha)}$ *remains a division algebra when extended to the real field K.* We have the parallel decompositions of

$$A \text{ into } \vartheta_\alpha E\ , \qquad Q \text{ into } Q_\alpha\ , \qquad L \text{ into } L_\alpha$$
$$[R \text{ into } R_\alpha\ , \qquad C \text{ into } C_\alpha\ , \qquad S \text{ into } S_\alpha]\ .$$

$\mathfrak{L}_\alpha$ is irreducible in $k(\vartheta_\alpha)$. Our remark proves that the commutator algebra $\mathfrak{Q}^{(\alpha)}$ of $\mathfrak{L}_\alpha$ in $k(\vartheta_\alpha)$ remains a division algebra *under extension to K* from which fact the criterion (1.3-D) permits drawing the inference that $\mathfrak{L}_\alpha$ *is irreducible in K.* Furthermore we should keep in mind that in $\mathfrak{Q}^{(\alpha)}$ our involution $q^{(\alpha)} \rightarrow q_*^{(\alpha)}$ consists in the transition from a quantic q to its "complex conjugate" q_* defined by:

$$(4.21) \qquad \begin{array}{c|c|c} q\ = q_0 & q\ = q_0 + q_1\iota & q\ = q_0 + q_1\iota_1 + q_2\iota_2 + q_3\iota_1 \\ q_* = q_0 & q_* = q_0 - q_1\iota & q_* = q_0 - q_1\iota_1 - q_2\iota_2 - q_3\iota_3 \end{array}$$

respectively. In each case we have

$$Q^{(\alpha)} = (q^{(\alpha)}) \times E_f\ .$$

MAIN THEOREM, FIRST PART. *A Riemann algebra $\mathfrak{L}$ splits over a certain totally real field $k(\vartheta)$ of degree $n = mv$ with its central field κ of degree v into parts of degree df which are irreducible in the real field K. It is described relatively to $k(\vartheta)$ by a quantic factor set where the algebra of quantics of order d is either scalar* ($d = 1$) *or a totally negative square root field* ($d = 2$), *or a totally negative quaternion* ($d = 4$).

[In cases II and III ascent to an absolute splitting field would be accomplished by adjoining the square root $\sqrt{-\lambda}$; we prefer, however, to stop at the totally real field $k(\vartheta)$.[8]

(4.3) Before going on we shall mention a few elementary features common to our three algebras $\mathfrak{q}_K$ of quantics q. The product of a q with its complex-conjugate q_*, (4.21), is a positive scalar $N(q)$, the *norm* of q:

$$N(q) = q_0^2 \quad | \quad q_0^2 + \lambda q_1^2 \quad | \quad q_0^2 + \lambda q_1^2 + \mu q_2^2 + \lambda\mu q_3^2,$$

which satisfies the multiplicative law:

$$N(pq) = N(p)\cdot N(q)\ .$$

[8] Albert adjoins to his Galois splitting field $k(\vartheta_1, \cdots, \vartheta_n)$ the extraneous real square roots $\sqrt{\lambda_\alpha}$, $\sqrt{\mu_\alpha}$ in order to make the case III more easily accessible; here we want to avoid the introduction of such irrationalities foreign to the problem.

After our algebra $\mathfrak{q}$ has been closed in K one may choose as "units"

$$\iota/\sqrt{\lambda} = i \quad | \quad \iota_1/\sqrt{\lambda} = i_1, \ \ \iota_2/\sqrt{\mu} = i_2$$

in cases II and III; one then has to deal with the Gauss field $K(i)$ and the ordinary Hamilton quaternions, respectively. An automorphism $q \rightarrow p$ in the latter case is expressed in terms of the units i_1, i_2, $i_3 = i_1 i_2$ by equations:

$$\begin{aligned} i_1 &\rightarrow a + a_1 i_1 + a_2 i_2 + a_3 i_3 = j_1, \\ i_2 &\rightarrow b + b_1 i_1 + b_2 i_2 + b_3 i_3 = j_2, \qquad \text{(all } a, b, c \text{ real numbers)} \\ i_3 &\rightarrow c + c_1 i_1 + c_2 i_2 + c_3 i_3 = j_3 . \end{aligned}$$

The requirement $j_1^2 = -1$ yields:

$$a^2 - a_1^2 - a_2^2 - a_3^2 = -1 \ ; \qquad 2aa_1 = 2aa_2 = 2aa_3 = 0 \, .$$

Since simultaneous vanishing of a_1, a_2, a_3 would contradict the first equation, we must have $2a = 0$ and for the same reason $2b = 0$, $2c = 0$. This means that the automorphism $q \rightarrow p$ carries q_* into p_*. Consequently the norm $N(q)$ is left invariant. Adding the simpler cases I and II we may state our result in the following

LEMMA (4.3-A). *An isomorphism T between α- and β-quantics matches $q_*^{(\alpha)} \leftrightarrow q_*^{(\beta)}$ as well as $q^{(\alpha)} \leftrightarrow q^{(\beta)}$. It leaves the norm invariant: $N_\alpha(q^{(\alpha)}) = N_\beta(q^{(\beta)})$.*

In computing explicitly the multiplication $(q) : x' = qx$ in our quaternion algebra, one finds

$$(4.31) \qquad (q) = \left\| \begin{matrix} q_0, & -\lambda q_1, & -\mu q_2, & -\lambda\mu q_3 \\ q_1, & q_0, & -\mu q_3, & \mu q_2 \\ q_2, & \lambda q_3, & q_0, & -\lambda q_1 \\ q_3, & -q_2, & q_1, & q_0 \end{matrix} \right\|$$

and we verify the relation

$$(q_*)' = (n)(q)(n)^{-1}$$

where

$$(4.32) \qquad (n) = \left\| \begin{matrix} 1 & & & \\ & \lambda & & \\ & & \mu & \\ & & & \lambda\mu \end{matrix} \right\|$$

is the coefficient matrix of the norm. It is important to observe that (n) is symmetric and positive-definite. Adding again the simpler cases I and II we thus proved

LEMMA (4.3-B):

(4.33) $$(q_*)' = (n)(q)(n)^{-1}$$

where (n) *is the coefficient matrix of the norm.*]

5. The Norm Condition

(5.1) Before attacking the slightly more difficult cases II and III we treat, as a model, case I where our totally real splitting field $k(\vartheta)$ splits $\mathfrak{L}$ into *absolutely* irreducible parts $\mathfrak{L}_\alpha$.

The equation

$$L'(l_*)C = CL(l)$$

defining the involution $l \to l_*$ of $\mathfrak{L}$ splits into the relations

(5.11) $$L'_\alpha(l_*) = C_\alpha L_\alpha(l)C_\alpha^{-1} .$$

We have

(5.12) $$L_\alpha A_{\alpha\beta} = A_{\alpha\beta}L_\beta .$$

The $\check{A}_{\alpha\beta} = A'^{-1}_{\alpha\beta}$ fulfill the same conditions with respect to the L'_α as the $A_{\alpha\beta}$ themselves relatively to the L_α and $C_\alpha A_{\alpha\beta}C_\beta^{-1}$ relatively to $C_\alpha L_\alpha C_\alpha^{-1}$. Hence (5.11) leads to a relation of the form

(5.13) $$\check{A}_{\alpha\beta} = e_{\alpha\beta}\cdot C_\alpha A_{\alpha\beta}C_\beta^{-1}$$

with a conjugate set of numbers $e_{\alpha\beta}$, or

(5.14) $$C_\beta = e_{\alpha\beta}\cdot A'_{\alpha\beta}C_\alpha A_{\alpha\beta} .$$

When we perform the transition from C_α to C_γ on the one hand directly in accordance with this equation, and on the other hand by passing through C_β, we find in making use, for the second process, of the equation

$$A_{\alpha\beta}A_{\beta\gamma} = c_{\alpha\beta\gamma}A_{\alpha\gamma}$$

that the skew-symmetric form C_γ is the transform $A'_{\alpha\gamma}C_\alpha A_{\alpha\gamma}$ of C_α multiplied by $e_{\alpha\gamma}$ on the one hand, or by $e_{\alpha\beta}e_{\beta\gamma}\cdot c^2_{\alpha\beta\gamma}$ on the other hand. Hence

(5.15) $$c^2_{\alpha\beta\gamma} = e_{\alpha\gamma}/e_{\alpha\beta}e_{\beta\gamma}\ (\sim 1) .$$

The numbers $e_{\alpha\beta}$ must be positive as is shown by the following simple observation. The $P_\alpha = C_\alpha L_\alpha$, because of (5.12), satisfy the same relation (5.14) as C_α:

(5.16) $$P_\beta = e_{\alpha\beta}\cdot A'_{\alpha\beta}P_\alpha A_{\alpha\beta}$$

if L lies in $\mathfrak{L}$ or its closure $\mathfrak{L}_K$. Since $CR = S$, $C_\alpha R_\alpha = S_\alpha$ we have in particular

(5.17) $$S_\beta = e_{\alpha\beta}\cdot A'_{\alpha\beta}S_\alpha A_{\alpha\beta} .$$

All quadratic forms S_α are positive definite. By the transformation $A_{\alpha\beta}$ the positive form S_α is carried into the positive form $A'_{\alpha\beta}S_\alpha A_{\alpha\beta}$. By (5.17) this coincides with the positive form S_β but for the factor $e_{\alpha\beta}$; hence this factor is to be positive. We have arrived at the following result:

The factor set $c_{\alpha\beta\gamma}$ of a Riemann algebra $\mathfrak{R}$ of type I *satisfies relations*

$$c^2_{\alpha\beta\gamma} = e_{\alpha\gamma}/e_{\alpha\beta}e_{\beta\gamma} \tag{5.15}$$

where $e_{\alpha\beta}$ is a double set of positive numbers conjugate over the central field κ. We say that c^2 is *totally positive equivalent* 1.

The condition is not only necessary but sufficient. *For let* (5.15) *be fulfilled.* These equations state that $\breve{A}_{\alpha\beta}$ has the same factor set as $e_{\alpha\beta}A_{\alpha\beta}$, and we know by proposition 2) in (3.4) that from this an equivalence like (5.13) follows with some conjugate non-singular matrices C_α. We constructed such a C_α, cf. (3.44), by means of the formula

$$C_\alpha = \sum_\rho \zeta_\rho e_{\rho\alpha} \breve{A}^{-1}_{\rho\alpha} A_{\rho\alpha} = \sum_\rho \zeta_\rho e_{\rho\alpha} A'_{\rho\alpha} A_{\rho\alpha}$$

where ζ is a number in $k(\vartheta)$. Let us take ζ in particular as a square number $\zeta = \xi^2$, ξ in $k(\vartheta)$, so that ζ is totally positive. The coefficients $e_{\rho\alpha}$ are positive by assumption. $A'A$ is a positive symmetric matrix if A is real; it is indeed the transform of the unit matrix E by the transformation A. *Hence our*

$$C_\alpha = \sum_\rho e_{\rho\alpha}\zeta_\rho A'_{\rho\alpha}A_{\rho\alpha} \qquad (\zeta_\rho > 0) \tag{5.18}$$

is symmetric, positive, and therefore non-singular; no special precautions against possible degeneration are necessary. This is the essential part of the proof of sufficiency; it needs some elementary supplement which the last section will take care of, but the pivot of our whole demonstration consists in the two formulas (5.17), (5.18), the first proving (5.15) and $e_{\alpha\beta} > 0$ to be a necessary condition, the second warranting the existence of a symmetric positive C, once this condition is fulfilled.

(5.2) It is easy to survey the *modifications needed to adapt our considerations to the other cases* II *and* III. As a consequence of

$$A_{\alpha\beta}L_\beta = L_\alpha A_{\alpha\beta}$$

we have

$$\breve{A}_{\alpha\beta}L'_\beta(l) = L'_\alpha(l)\breve{A}_{\alpha\beta}.$$

Hence $C_\alpha^{-1}\breve{A}_{\alpha\beta}C_\beta$ have the same significance for $C_\alpha^{-1}L'_\alpha(l)C_\alpha = L_\alpha(l_*)$ and therefore

$$C_\alpha^{-1}\breve{A}_{\alpha\beta}C_\beta = Q^{(\alpha)}A_{\alpha\beta}(= q^{(\alpha)}A_{\alpha\beta}) \qquad [Q^{(\alpha)} \text{ in } \mathfrak{Q}^{(\alpha)}]$$

or

$$C_\beta = A'_{\alpha\beta}C_\alpha Q^{(\alpha)}A_{\alpha\beta}. \tag{5.21}$$

We must try to prove that $q^{(\alpha)}$ is a scalar. Putting the $'$ on the whole equation (5.21) we get because of $C'_\alpha = \pm C_\alpha$:

$$C_\beta = A'_{\alpha\beta} Q^{(\alpha)\prime} C_\alpha A_{\alpha\beta}$$

which changes by

$$C_\alpha^{-1} Q^{(\alpha)\prime} C_\alpha = Q_*^{(\alpha)} \tag{5.22}$$

into

$$C_\beta = A'_{\alpha\beta} C_\alpha Q_*^{(\alpha)} A_{\alpha\beta}.$$

Comparison with (5.21) shows that $q_*^{(\alpha)} = q^{(\alpha)}$, and hence $q^{(\alpha)}$ is a scalar. We denote it by $e_{\alpha\beta}$ as before, and then obtain the equations (5.14), (5.17) with their implication $e_{\alpha\beta} > 0$.

Let us write the equation

$$A_{\alpha\beta} A_{\beta\gamma} = c_{\alpha\beta\gamma}^{(\alpha)} A_{\alpha\gamma}$$

in which $c_{\alpha\beta\gamma}^{(\alpha)}$ stands for the matrix $Q^{(\alpha)}$ corresponding to the α-quantic $q^{(\alpha)} = c_{\alpha\beta\gamma}^{(\alpha)}$ in the form

$$A_{\alpha\beta} A_{\beta\gamma} = Q^{(\alpha)} A_{\alpha\gamma}.$$

If we now proceed as before we find on the one hand

$$C_\gamma = e_{\alpha\gamma} \cdot A'_{\alpha\gamma} C_\alpha A_{\alpha\gamma}$$

and on the other

$$C_\gamma = e_{\alpha\beta} e_{\beta\gamma} A'_{\alpha\gamma} Q^{(\alpha)\prime} C_\alpha Q^{(\alpha)} A_{\alpha\gamma}.$$

Making use again of (5.22) the middle factors

$$Q^{(\alpha)\prime} C_\alpha Q^{(\alpha)} \text{ change into } C_\alpha Q_*^{(\alpha)} Q^{(\alpha)} = N(q^{(\alpha)}) C_\alpha,$$

and our result is

$$N(q^{(\alpha)}) = \frac{e_{\alpha\gamma}}{e_{\alpha\beta} e_{\beta\gamma}}.$$

For its full appreciation one should observe that (3.57), (3.58) by the multiplicative property of the norm and lemma (4.3-A) imply

$$N(c_{\alpha\beta\gamma}^{(\alpha)}) = N(c_{\alpha\beta\gamma}^{(\gamma)});$$

$$N(c_{\alpha\beta\gamma}^{(\alpha)}) \cdot N(c_{\alpha\gamma\delta}^{(\alpha)}) = N(c_{\alpha\beta\delta}^{(\delta)}) \cdot N(c_{\beta\gamma\delta}^{(\delta)}).$$

This means that *the norm of a quantic factor set of types* I, II *or* III *is a scalar factor set.* We have ascertained the following necessary condition, that the algebra described by a quantic factor set of this type relatively to $k(\vartheta)$, be a Riemann algebra:

The norm of the factor set must be totally positive equivalent 1.

(5.3) Vice versa, *if this condition prevails* we proceed to the construction of a pure Riemann matrix associated with $\mathfrak{K}$ in the following way. The first step is to define an anti-automorphic involution in $\mathfrak{K}$ by an appropriately chosen C. From the matrix (n) mentioned in Lemma (4.3-B) and its conjugates (n_α) we form $(n_\alpha) \times E_f = N_\alpha$ and then put

$$C_\alpha = \sum_\rho e_{\rho\alpha} \zeta_\rho A'_{\rho\alpha} N_\rho A_{\rho\alpha}. \tag{5.31}$$

ζ is a totally positive number in $k(\vartheta)$, $\zeta_\rho > 0$; for instance, we choose $\zeta = \xi^2$, ξ in $k(\vartheta)$. $e_{\rho\alpha}$ is >0, and $A'_{\rho\alpha}N_\rho A_{\rho\alpha}$ is the symmetric positive N_ρ transformed by $A_{\rho\alpha}$; each term of our sum (5.31) and consequently the whole sum is symmetric and positive. C is the rational matrix that breaks up into the conjugate C_α. We are going to prove that C_α fulfills the conditions required:

$$Q^{(\alpha)\prime} C_\alpha = C_\alpha Q_*^{(\alpha)}, \tag{5.32}$$

$$C_\beta = e_{\alpha\beta} \cdot A'_{\alpha\beta} C_\alpha A_{\alpha\beta}. \tag{5.33}$$

The relation

$$Q^{(\rho)} A_{\rho\alpha} = A_{\rho\alpha} Q^{(\alpha)} \tag{5.34}$$

defines the isomorphism $T_{\rho\alpha}$: $q^{(\rho)} \leftrightarrow q^{(\alpha)}$. By Lemma (4.3-A), one has at the same time

$$Q_*^{(\rho)} A_{\rho\alpha} = A_{\rho\alpha} Q_*^{(\alpha)},$$

while (5.34) yields

$$A'_{\rho\alpha} Q^{(\rho)\prime} = Q^{(\alpha)\prime} A'_{\rho\alpha}.$$

Therefore

$$C_\alpha Q_*^{(\alpha)} = \sum_\rho e_{\rho\alpha} \zeta_\rho A'_{\rho\alpha} N_\rho Q_*^{(\rho)} A_{\rho\alpha},$$

$$Q^{(\alpha)\prime} C_\alpha = \sum_\rho e_{\rho\alpha} \zeta_\rho A'_{\rho\alpha} Q^{(\rho)\prime} N_\rho A_{\rho\alpha};$$

their coincidence results from the equation (4.33) or

$$Q^{(\rho)\prime} = N_\rho Q_*^{(\rho)} N_\rho^{-1}. \tag{5.35}$$

The right side of (5.33) is by definition

$$\sum_\rho e_{\rho\alpha} e_{\alpha\beta} \zeta_\rho (A_{\rho\alpha} A_{\alpha\beta})' N_\rho (A_{\rho\alpha} A_{\alpha\beta}). \tag{5.36}$$

After putting again

$$c^{(\rho)}_{\rho\alpha\beta} = q^{(\rho)}$$

we have

$$A_{\rho\alpha} A_{\alpha\beta} = Q^{(\rho)} A_{\rho\beta}.$$

This changes the matrix under the sum at the right side of (5.36) into

$$A'_{\rho\beta}Q^{(\rho)\prime}N_\rho Q^{(\rho)}A_{\rho\beta}.$$

According to (5.35),

$$Q^{(\rho)\prime}N_\rho Q^{(\rho)} = N_\rho Q_*^{(\rho)}Q^{(\rho)} = N(q^{(\rho)})\cdot N_\rho.$$

By assumption

$$e_{\rho\alpha}e_{\alpha\beta}N(q^{(\rho)}) = e_{\rho\beta},$$

and thus (5.33) has been verified.

6. Main Theorem

(6.1) The $C_\alpha = C(\vartheta_\alpha)$, as constructed in the last section are the conjugate parts of a rational C. By means of

$$L'(l_*) = CL(l)C^{-1} \qquad L'_\alpha(l_*) = C_\alpha L_\alpha(l)C_\alpha^{-1}$$

it defines an anti-automorphic involution $l \rightarrow l_*$ in $\mathfrak{l}$. Indeed, owing to (5.32) and (5.33), the parts M_α of the rational matrix M defined by

$$M' = CLC^{-1}, \qquad M'_\alpha = C_\alpha L_\alpha C_\alpha^{-1}$$

satisfy the relations

$$M_\alpha A_{\alpha\beta} = A_{\alpha\beta}M_\beta$$

and commute with all $Q^{(\alpha)}$ (or $Q_*^{(\alpha)}$) as well as the L_α. M therefore lies in $\mathfrak{L}$, according to Lemma (3.5). $l \rightarrow l_*$ is involutorial because of the symmetry of C.

Our C may now be called C_0 and we write $C_0(\vartheta)$ instead of $C(\vartheta)$. The terms *even* and *odd* refer to the involution $l \rightarrow l_*$ generated by C_0. Let $\mathfrak{L}^+(\mathfrak{L}^-)$ be the linear k-set of even (odd) elements in $\mathfrak{L}$. The even elements in the extension $\mathfrak{L}_K$ form the extension $\mathfrak{L}_K^+$ of $\mathfrak{L}^+$ to K. Indeed L being an even element in $\mathfrak{L}_K$:

$$L = \sum_i z_i L^{(i)} \tag{6.11}$$

(z_i real numbers, $L^{(i)}$ a base of $\mathfrak{L}$) we obtain by addition of the starred equation to (6.11):

$$2L = \sum_i z_i(L^{(i)} + L_*^{(i)}).$$

The same remark applies to the odd elements of $\mathfrak{L}$ and $\mathfrak{L}_K$. *Let*

$$L^{(i)} \ (i = 1, 2, \cdots, \nu)$$

now be a base of $\mathfrak{L}^+$, and in particular $L^{(1)} = E$.

If we chose C_0 as our C we would obtain *even* Riemann matrices alone. We therefore put

$$C = C_0L_0, \qquad S = C_0L[z]$$

where L_0 is an even or odd non-singular matrix in $\mathfrak{L}$ and $L[z]$ lies in $\mathfrak{L}^+_K$:

$$L[z] = z_1 L^{(1)} + z_2 L^{(2)} + \cdots + z_\nu L^{(\nu)}.$$

$$R = C^{-1}S = L_0^{-1}L[z]$$

shall be our Riemann matrix. We first choose the real numbers z_i so that there exists no homogeneous linear relation among them with rational coefficients.[9] We may normalize $z_1 = 1$. The equation

$$S = C_0 + z_2 \cdot C_0 L^{(2)} + \cdots$$

shows S to be positive definite provided $z_2, \cdots, z_\nu$ are sufficiently small. This can be taken care of[9] without violating the linear independence of the z_i in k by multiplying $z_2, \cdots, z_\nu$ with a common, sufficiently-small, rational factor $\neq 0$.

After the positive character of S is secured, the next question is about the rational commutators A of R. Such a matrix A must commute with all elements $L_0^{-1}L^{(i)}$ which form the base of $L_0^{-1}\mathfrak{L}^+ = \Lambda$; therefore in particular with $L_0^{-1}L^{(1)} = L_0^{-1}$ and consequently with $L^{(i)}$ and with L_0. So we must try to prove the

Lemma (6.1): *A matrix A commuting with L_0 and the even elements of $\mathfrak{L}$ (or $\mathfrak{L}_K$) commutes with all elements of $\mathfrak{L}$ (or $\mathfrak{L}_K$).*

$L_0^{-1}\mathfrak{L}^+ = \Lambda$ is obviously the linear k-set associated with our R. If L^+ is in $\mathfrak{L}^+$ so is $L_0^{-1}L^+L_0$; hence $\Lambda = \mathfrak{L}^+L_0^{-1}$, and the involution $L \rightarrow L_*$ carries Λ into itself. Λ contains $L_0 = L_0^{-1}L_0^2$; the algebraic closure of Λ—which is the associated algebra of R—thus embraces $\mathfrak{L}^+$ and is either the algebraic closure $(\mathfrak{L}^+)$ of $\mathfrak{L}^+$ or [if L_0^{-1} is not in $(\mathfrak{L}^+)$] the sum of $(\mathfrak{L}^+)$ and $L_0^{-1}(\mathfrak{L}^+)$.

The lemma (6.1) once established, we may be sure that Λ and hence R are rationally *irreducible*. Because Λ is invariant with respect to the involution and C_0 is positive definite, *reduction* of Λ would result in rational *decomposition* according to the proof of Theorem (2.2-B). The matrix, equal to the unit in the one and to zero in the other partial space, would then be a commutator of Λ without being a commutator of $\mathfrak{L}$; for a non-vanishing commutator of $\mathfrak{L}$ is non-singular. The algebraic closure $(\mathfrak{L}^+)$ or $(\mathfrak{L}^+) + L_0^{-1}(\mathfrak{L}^+)$ of Λ must coincide with $\mathfrak{L}$.

(6.2) We split by means of our totally real $k(\vartheta)$ and afterwards extend the individual $\mathfrak{L}_\alpha = \mathfrak{L}(\vartheta_\alpha)$ to K. To prove the lemma (6.1) we must show two things:

1) A matrix $A_{\alpha\beta}$ satisfying the relation

$$A_{\alpha\beta}L_\beta^+ = L_\alpha^+ A_{\alpha\beta}$$

for all L^+ in $\mathfrak{L}^+$ (or $\mathfrak{L}^+_K$) must needs be zero provided α and β are not coördinated.

2) A real matrix A_α commuting with the element $L_0(\vartheta_\alpha)$ and the even $L_\alpha^+ = L^+(\vartheta_\alpha)$ in $\mathfrak{L}_\alpha$ commutes with all L_α.

[9] When one analyzes the assumptions as to the relation between K and k on which this simple construction depends, one finds this: the ring of all numbers in K that are dominated by k is to form a linear k-set *of infinite order* (or at least of order $\geq g^2$). Here a number α in K may be said to be dominated by k provided there exists a number α_0 in k such that $|\alpha| < \alpha_0$. Choose $z_2, \cdots, z_\nu$ as numbers in the ring just mentioned!

As to 1), we observe that the matrix L defined by

$$L_\alpha = \eta_\alpha E \qquad (\eta_\alpha \text{ real number})$$

lies in $\mathfrak{L}_K$ according to the criterion, Lemma (3.5), if $\eta_\alpha = \eta_\beta$ holds for each pair of coördinated indices α, β (it lies even in $\mathfrak{L}$ when the η_α are the conjugates of a number η in the central field κ). The matrix L thus defined is *even*. Hence the assumption concerning $A_{\alpha\beta}$ implies the equation

$$(\eta_\alpha - \eta_\beta)A_{\alpha\beta} = 0.$$

Operating in $\mathfrak{L}_K$ one may choose $\eta_\alpha = 1$, $\eta_\beta = 0$ provided α and β are not coördinated; if one prefers to stay within $\mathfrak{L}$ one would take a determining number of $\kappa = k(\eta)$ for η and then have $\eta_\alpha \neq \eta_\beta$ under the same assumption. In either way one gets the desired result: $A_{\alpha\beta} = 0$.

Point 2) needs more careful consideration. We replace ϑ_α by the indeterminate root ϑ and for brevity's sake then suppress the argument ϑ (or the index α). With L ranging over all elements of $\mathfrak{L}_K(\vartheta)$, $C_0L = P$ varies over a linear set $\mathfrak{P}$. To the *even* L corresponds the *symmetric* P. The assumption that A commutes with L amounts to the relation

$$BP = PA \tag{6.21}$$

for the corresponding P when we put $C_0AC_0^{-1} = B$. Requiring (6.21) to hold for every symmetric P in $\mathfrak{P}$, makes superfluous the explicit statement of this link between the constant matrices A and B: $BC_0 = C_0A$, as it is included in (6.21) for $L = E$, $P = C_0$. However, we have to add the one equation

$$BP^0 = P^0A \tag{6.22}$$

corresponding to the fixed element $P^0 = C = C_0L_0$. Our concern is to ascertain that two matrices A, B satisfying (6.21) for P^0 and every *symmetric* P in $\mathfrak{P}$ satisfy (6.21) for every P in $\mathfrak{P}$.

Let q be our quantics forming the division algebra $\mathfrak{q}$ of order $d = 1, 2$ or 4, over K, and $Q = (q) \times E_f$. Each matrix $P = C_0L$, L in $\mathfrak{L}_K(\vartheta)$, satisfies the equation

$$Q'_*P = PQ; \tag{6.23}$$

and vice versa, a P satisfying (6.23) for each q must needs be $= C_0L$ where L commutes with each Q and hence belongs to the algebra $\mathfrak{L}_K(\vartheta)$. By the way, $\mathfrak{L}_K(\vartheta)$ is the algebra $(\mathfrak{q}')_f$ and each P may be written as NL where $N = (n) \times E_f$ is the constant "norm matrix" (4.32). In either way we find that the linear K-set $\mathfrak{P}$ consists of all matrices of the following form in the three cases $d = 1$, 2, 4, respectively:

$$P_0, \qquad \left\| \begin{matrix} P_0, & -P_1 \\ P_1, & \lambda P_0 \end{matrix} \right\|, \qquad \left\| \begin{matrix} P_0, & -P_1, & -P_2, & -P_3 \\ P_1, & \lambda P_0, & P_3, & -\lambda P_2 \\ P_2, & -P_3, & \mu P_0, & \mu P_1 \\ P_3, & \lambda P_2, & -\mu P_1, & \lambda\mu P_0 \end{matrix} \right\| \tag{6.24}$$

where P_0 or P_0, P_1 or P_0, P_1, P_2, P_3 are arbitrary real matrices of degree f. This is in agreement with the order $df^2 = f^2, 2f^2, 4f^2$. Such a P is *symmetric* provided P_0 is symmetric and P_1, P_2, P_3 are skew-symmetric. The question can now be settled by the following trivial

Lemma (6.2). Two matrices A and B of degree f satisfying the equation $BX = XA$ for all symmetric X are of necessity the same multiple $A = B = \alpha E$ of the unit matrix, and hence satisfy the same equation for all X whatsoever.

Proof: $X = E$ yields

$$B = A = \| a_{ik} \| .$$

With a diagonal matrix X of the elements $x_{ii} = x_i$ one gets

$$a_{ik} x_k = x_i a_{ik};$$

hence if $i \neq k$ by choosing $x_i = 1$, $x_k = 0$: $a_{ik} = 0$. Consequently A is a diagonal matrix of the elements $a_{ii} = a_i$. We finally obtain with an arbitrary symmetric $X = \| x_{ik} \|$:

$$(a_i - a_k) x_{ik} = 0,$$

therefore $a_i = a_k$.

In case I the lemma settles our question at once: the validity of (6.21) for all symmetric P's implies the same for all P's whatsoever. In case II and III we write

$$A = \| A_{ik} \|, \qquad (i, k = 0, 1 \text{ or } 0, 1, 2, 3)$$

the same for B, and

$$\lambda_0 = 1, \lambda_1 = \lambda \mid \lambda_0 = 1, \lambda_1 = \lambda, \lambda_2 = \mu, \lambda_3 = \lambda\mu .$$

We first take P_1 $(= P_2 = P_3) = 0$ and obtain the equations

$$B_{ik} \lambda_k P_0 = P_0 \lambda_i A_{ik} \tag{6.25}$$

holding for every symmetric P_0. Our lemma shows that therefore

$$A_{ik} = \alpha_{ik} E_f , \qquad B_{ik} = \beta_{ik} E_f$$

are multiples of the unit matrix, the real numbers α_{ik}, β_{ik} satisfying

$$\lambda_i \alpha_{ik} = \lambda_k \beta_{ik} .$$

Hence the equations (6.25) hold for every P_0 whatsoever. If we now consider the equation (6.21) for those P, (6.24), in which $P_0 = 0$ and if we treat P_1, P_2, P_3 as independent matrices, we find a certain number of equations

$$\alpha P_i = \beta P_i \qquad (i = 1 \text{ or } i = 1, 2, 3) \tag{6.26}$$

where α and β are numbers. They are required to hold good for an arbitrary anti-symmetric P_i. *If* $f > 1$ there exist anti-symmetric matrices $\neq 0$ and thus (6.26) implies $\alpha = \beta$; but then (6.26) holds for every P_i whatsoever, and we thus made sure that validity of (6.21) for symmetric P's implies the same for all P's. *The case* $f = 1$ *is different.* Here we have only *one* independent symmetric P, and thus $\mathfrak{L}_K^+(\vartheta)$ consists of the multiples of the unit matrix alone, and so does its algebraic closure $(\mathfrak{L}_K^+(\vartheta))$. In case II, $f = 1$, one is forced to choose L_0 odd and the corresponding $P^0 = C = C_0L_0$ antisymmetric. Else (6.21) for all symmetric P's together with (6.22) would be bound to have more solutions than the equation (6.21) when required for *all* P's. In case III, $f = 1$, even this trick will not help us out of the trap. For even with an odd $L_0(\vartheta)$ the sum $(\mathfrak{L}_K^+(\vartheta)) + L_0^{-1}(\vartheta)(\mathfrak{L}_K^+(\vartheta))$ is of order 2 rather than of order 4, as it should be.

(6.3) The question whether there exists an odd *non-singular* $L_0(\vartheta)$ is to be discussed. In case I this is only possible for an *even* f. But for $d = 1, f$ even, or $d = 2$ or $d = 4$, (6.24) at once allows writing down a non-singular antisymmetric P and hence an odd $L_0(\vartheta)$ lying in the extension $\mathfrak{L}_K^-(\vartheta)$. The parts $L_\alpha = L_0(\vartheta_\alpha)$ and L_β corresponding to non-coördinated α and β may be chosen independently whereas for coördinated indices L_β is to be taken as $A_{\alpha\beta}^{-1}L_\alpha A_{\alpha\beta}$, or P_β as $e_{\alpha\beta}\cdot A'_{\alpha\beta}P_\alpha A_{\alpha\beta}$; one thus obtains an odd non-singular L_0 in $\mathfrak{L}_K$. If one expresses the unsplit L_0 in terms of a base of $\mathfrak{L}^-$ with certain real coefficients y, one sees that $|L_0|$ is not identically zero in the variables y. One therefore may ascertain rational values of the y for which $|L_0| \neq 0$; this L_0 is then an odd non-singular matrix of $\mathfrak{L}$. We summarize our construction in the

MAIN THEOREM, SECOND PART. *When the Riemann algebra $\mathfrak{L}$ is described over a totally real splitting field $k(\vartheta)$ by means of a quantic factor set of the kind defined in the first part of the Main Theorem, then the norm of the factor set must be totally positive equivalent* 1. *This condition is not only necessary but also sufficient for $\mathfrak{L}$ to be associated with an even or odd pure Riemann matrix, save for the following limitations*:

$d = 1, f$ *odd*	$d = 2, f = 1$	$d = 4, f = 1$
no odd,	*no even,*	*neither an odd* *nor an even,*

associated Riemann matrix exists.

We must return for a moment to the investigation of necessary rather than sufficient conditions in order to determine whether these limitations lie in the nature of things and are not merely due to a lack of skill in our construction. To this end we have to consider that by Rosati's lemma (4.1), C necessarily decomposes into non-singular C_α's. The involution $q \rightarrow q_*$ effected by C_α in the realm of α-quantics is prescribed, hence $C(\vartheta)$ must be $= C_0(\vartheta)L(\vartheta)$ where $L(\vartheta)$ commutes with all $Q(\vartheta)$ and therefore must come to lie in $\mathfrak{L}(\vartheta)$ after $\mathfrak{L}(\vartheta)$ has been extended to $k(\vartheta)$. This leaves us no loophole.

7. Appendix. Automorphisms.

The scheme A as well as B, (1.34), may thus be described: it is a checkered square table with rows and columns labeled by a double index $i\alpha$ and $k\beta$ each field of which is occupied by a d-rowed matrix $A_{i\alpha,k\beta}$. If E_{ik} denotes the unit or zero matrix according as $i = k$ or $i \neq k$ we have more precisely

$$(7.1) \qquad A_{i\alpha,k\beta} = A_{ik}E_{\alpha\beta}, \qquad B_{i\alpha,k\beta} = E_{ik}B_{\alpha\beta}.$$

Let us return for a moment to the irreducible representation $\mathfrak{A}$: $a \rightarrow A = A(a)$ of a simple algebra $\mathfrak{a}$. If an automorphism $a \rightarrow a^*$ of $\mathfrak{a}$ be given, then $a \rightarrow A(a^*) = A^*$ is a representation of $\mathfrak{a}$ as well as $\mathfrak{A}$: $a \rightarrow A(a)$ itself, and like any representation of the simple $\mathfrak{a}$ is equivalent to a multiple of $\mathfrak{A}$. The words "a multiple of" are to be canceled because of equality of degree g. Hence there exists a non-singular matrix H in k such that

$$(7.2) \qquad A^* = HAH^{-1}$$

for every A in $\mathfrak{A}$. This applies in particular

(α) to the full matric algebra $\mathfrak{M}_g$ consisting of all g-rowed matrices in k, and

(β) to the regular representation of a division algebra.

The same holds true for the *multiple* $s\mathfrak{A}$ of our irreducible $\mathfrak{A}$ which we now again call $\mathfrak{A} = \{A\}$: each automorphism $A \rightarrow A^*$ is of the type (7.2). The matrix H at the same time defines an automorphism $B \rightarrow B^*$ in the commutator algebra $\mathfrak{B}$: $B^* = HBH^{-1}$. So we are led to study *simultaneous* automorphisms $A \rightarrow A^*$, $B \rightarrow B^*$ in $\mathfrak{A}$ and $\mathfrak{B}$. A necessary condition that both are expressible in the form

$$(7.3) \qquad A^* = HAH^{-1}, \qquad B^* = HBH^{-1}$$

by the same non-singular constant H in k is their coincidence within the cross-cut $\mathfrak{Z}$ of $\mathfrak{A}$ and $\mathfrak{B}$, the so-called *centrum.* In formula (7.1) each A_{ik} varies over ($\mathfrak{d}'$), each $B_{\alpha\beta}$ over ($\mathfrak{d}$). An element A common to $\mathfrak{A}$ and $\mathfrak{B}$, must have $A_{ik} = J \cdot E_{ik}$ in (7.1) where J lies in ($\mathfrak{d}'$) and in ($\mathfrak{d}$):

$$J: x \rightarrow x' = j_1 x = x j_2$$

(j_1 and j_2 fixed elements, x variable in $\mathfrak{d}$). But $j_1 x = x j_2$ yields $j_1 = j_2$ by putting $x = e$, and $j = j_1 = j_2$ must commute with all elements x of $\mathfrak{d}$. The elements j of this kind form the *centrum* $\mathfrak{z}$ of $\mathfrak{d}$. *Let us first assume that* $\mathfrak{z}$ *is of order* 1, that only the numerical multiples of the unit element e commute with all elements x of the division algebra $\mathfrak{d}$.

We then maintain that the d^2 transformations

$$(7.4) \qquad x' = bxa$$

yield a base of the complete matric algebra $\mathfrak{M}_d$ if we let a and b run independently over a base of $\mathfrak{d}$. By Burnside's theorem this is true provided the multiples of the unit matrix are the only transformations J commuting with all these transformations (7.4), i.e. with all transformations of type $x' = bx$ and $x' = xa$. For the first reason such a J must be itself of the form $x' = xj_2$, for the second reason of the form $x' = j_1 x$ (j_1 and j_2 in $\mathfrak{d}$); hence $j_1 = j_2$ lies in the centrum of $\mathfrak{d}$ and is a multiple of e. The result is that the product $A_{11}B_{11}$ yields a full base for all d-rowed matrices when A_{11} ranges over a base for ($\mathfrak{d}'$) and B_{11} for ($\mathfrak{d}$). The product of two matrices A and B, (7.1), is given by

$$(AB)_{i\alpha, k\beta} = A_{ik} \cdot B_{\alpha\beta},$$

and from this formula in connection with the result just obtained we readily deduce that AB provides a full base for all g-rowed matrices ($g = dst$) if A runs over a base of $\mathfrak{A}$ and B of $\mathfrak{B}$. This is in keeping with the orders $d \cdot t^2$ of $\mathfrak{A}$ and $d \cdot s^2$ of $\mathfrak{B}$; for their product equals $(dst)^2 = g^2$.

The two arbitrary given automorphisms $A \rightarrow A^*$, $B \rightarrow B^*$ define therefore (remembering that the A's commute with the B's!) an automorphism $AB \rightarrow A^*B^*$ of the full matric algebra $\mathfrak{M}_g$ and consequently statement (α) above assures us of the existence of a constant non-singular matrix H such that $A^*B^* = HABH^{-1}$, in particular (A or $B = E$):

$$A^* = HAH^{-1}, \qquad B^* = HBH^{-1}.$$

H is unambiguously determined, but for a numerical factor.

When we combine the identical automorphism of $\mathfrak{B}$ with a given automorphism $A \rightarrow A^*$ of $\mathfrak{A}$, our H commutes with every B and hence lies in $\mathfrak{A}$: *Every automorphism of* $\mathfrak{A}$ *is an inner automorphism.*[10]

If the centrum $\mathfrak{z}$ of $\mathfrak{d}$ is of order δ we may consider $\mathfrak{d}$ as a division algebra of order d/δ over the *field* $\mathfrak{z}$. Operating in this field throughout and finally replacing again each "number" j of this field by the δ-rowed matrix that represents it in the regular representation of $\mathfrak{z}$, we carry over our result to each pair of automorphisms $A \rightarrow A^*$, $B \rightarrow B^*$ in $\mathfrak{A}$ and $\mathfrak{B}$ which coincide with the identity for the elements Z common to $\mathfrak{A}$ and $\mathfrak{B}$. Application of the statement (β) above to the commutative division algebra $\mathfrak{z}$ enables us to weaken this restricting hypothesis to the assumption that both automorphisms coincide among each other for the elements Z of $\mathfrak{Z}$:

THEOREM. *Two automorphisms* $A \rightarrow A^*$, $B \rightarrow B^*$ *of* $\mathfrak{A}$ *and* $\mathfrak{B}$ *when coinciding within the centrum or cross-cut* $\mathfrak{Z}$ *of* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are generated by the same non-singular matrix H according to* (7.3). *In particular, each automorphism of* $\mathfrak{A}$ *which leaves invariant the elements of* $\mathfrak{Z}$ *is an inner automorphism.*

It is in no way unnatural that the proof first deals with the case of a "normal" algebra whose centrum does not reach beyond the reference field k. For what ambiguity there is in H comes from the centrum: the unruly things happen in the commutative fields, the whole superstructure of algebras is of a comparatively simple nature.

THE INSTITUTE FOR ADVANCED STUDY

[10] Skolem, "Zur Theorie der assoziativen Zahlensysteme," *Skr. Norske Vid.-Akad.*, Oslo (1927), pp. 21, 22; R. Brauer, *Math. Zeitschrift*, vol. **30** (1929), p. 105.