SOME RESULTS IN THE THEORY OF LINEAR NON-ASSOCIATIVE ALGEBRAS

BY

RICHARD H. BRUCK

1. **Introduction.** In order to make the present paper reasonably self-contained, it would be necessary both to repeat in detail portions of papers by N. Jacobson [1][1], A. A. Albert [2, 3], and the author [4] and to list a number of results from the theory of representations and of linear associative algebras. On the whole we have done neither. Nevertheless, we have given references to the somewhat scattered literature of linear non-associative algebras whenever it has seemed desirable to do so.

With two unimportant exceptions we use Albert's notation [2] in regard to linear transformations. We prefer the older form x^T to Albert's more recent notation xT, and, moreover, we make no essential distinction in general between a linear transformation T and its matrix relative to a given basis. Lest there should be any ambiguity in regard to the form of the matrix the reader is asked to think of x as a row-vector and of T as a square matrix multiplying x on the right.

Two linear algebras $\mathfrak{A}$, $\mathfrak{A}_o$ are said to be *isotopic* if they consist of the same elements, and if there exist three nonsingular linear transformations U, V, W such that $xoy=(x^U \cdot y^V)^W$, where xoy, $x \cdot y$ designate the ordered product of x and y in $\mathfrak{A}_o$ and $\mathfrak{A}$ respectively. In particular $\mathfrak{A}_o$ is a *principal isotope* of $\mathfrak{A}$ if we can choose $W=I$, $xoy=x^U \cdot y^V$. It may be shown that every isotope of $\mathfrak{A}$ is isomorphic to a principal isotope. (These definitions are evidently distinct from but equivalent to those of Albert; see [4, footnote 3].)

An essential feature of the paper is the construction of a variety of simple algebras of every finite order and also of infinite order; some of these in particular are division algebras. It should be noted that all the simple algebras defined by A. A. Albert [2, II] are of composite order and possess a unit element. We proceed to outline the contents of the paper in greater detail.

In §2, with the help of a lemma which has apparently been neglected heretofore (Lemma 2B) we give an adequate treatment of *right-simple* algebras (those without proper right ideals). Moreover, we show (Theorem 2C) that if a linear algebra $\mathfrak{A}$ possesses a unit element, then, regardless of the nature of the underlying field and of the (finite) order of $\mathfrak{A}$, the algebra has an isotope which is simple. It is thus natural to introduce the notion of an *isotopically simple* algebra, namely a simple algebra every isotope of which is simple.

Presented to the Society, November 27, 1943; received by the editors February 10, 1944.

[1] Numbers in square brackets designate references to the literature which will be found at the end of the paper.

In §3 we prove (Theorem 3C) that every algebra $\mathfrak{A}$ has an isotope $\mathfrak{B}$ with a composition series

$$\mathfrak{B} = \mathfrak{B}_0 \supset \mathfrak{B}_1 \supset \mathfrak{B}_2 \supset \cdots \supset \mathfrak{B}_k = (0), \tag{1.1}$$

where, for each i of the range $1, 2, \cdots, k$, $\mathfrak{B}_i$ is an ideal of $\mathfrak{B}_{i-1}$ and the difference algebra $\mathfrak{C}_i \equiv \mathfrak{B}_{i-1} = \mathfrak{B}_i$ is isotopically simple. Since the extension problem for non-associative algebras offers no difficulty we have in a sense reduced the theory of linear non-associative algebras to the study of isotopically simple algebras.

We divide algebras into four convenient classes, and prove by direct construction that, regardless of the underlying field, there exist isotopically simple algebras of class I for every order $n \neq 2$, and of class II or III for every order $n > 3$.

The algebras of class IV, characterized by the fact that every element is a two-sided divisor of zero, offer a good deal of difficulty in regard to the question of isotopic simplicity, and are considered at some length in §4 from the standpoint of the theory of trilinear forms. In particular it is shown that the Lie algebra of order $n(n-1)/2$, consisting of all skew-symmetric matrices (over a real field) under the commutator product $AoB = AB - BA$, is isotopically simple (Theorem 4E). We also give a criterion for division algebras which does not seem to be in the literature (Theorem 4A, Lemma 4A).

In §5 the concept of *isotopic indecomposability* is introduced and briefly discussed, and §6 treats the notion of a *quasigroup algebra*. §7 is devoted to the theory of *quasigroup rings* (linear closures of finite quasigroups over a field F) and these are shown to be semi-simple under hypotheses which are satisfied in particular when F is non-modular (Theorem 7A). Theorem 7A is essentially due to D. C. Murdoch. In §8 (Theorem 8A) it is shown that, corresponding to every I.P. (inverse property) loop of finite order $n > 2$ and to every underlying field except $GF(2)$, there exists a quasigroup algebra of order n, with a unit element, which is both right-simple and left-simple. Finally, §9 is concerned with the definition and construction of a type of simple algebra called a *truncated loop algebra*, which exists for every finite order n.

Because of its applications to the theory of linear algebras we consider in §10 the theory of quasigroup extensions. If H is an arbitrary set of finite or transfinite order m and if Q is any quasigroup of finite or transfinite order n we define a quasigroup $R = (H, Q)$ of order mn, an *extension* of H by Q, with the essential property that R is homomorphic to Q. Conversely, if any quasigroup R is homomorphic to a quasigroup Q then there exists a set H such that R is isomorphic to an extension (H, Q). This theory is compared and linked with Albert's extension theory [3, II] for loops. In §11 we define a *generalized quasigroup* algebra by extending a linear vector space by a quasigroup in such a manner as to preserve linearity; however, the nonzero elements of the resultant algebra do not in general form a quasigroup under multiplication, so that the analogy with quasigroup extension is incomplete.

The remaining sections of the paper are devoted to division algebras and division rings, that is, to rings and linear algebras whose nonzero elements form a quasigroup under multiplication. §12 treats a type of division ring, a so-called *generalized Hilbert* ring of infinite order over a field, and §13 mentions several other methods of constructing non-associative division rings of infinite order. §14 supplies a useful criterion that two division algebras should be non-isotopic. In §15 there is given a brief account of certain quasigroup algebras, of orders 4 and 8 over the field of reals, which are division algebras. (Although these algebras of order 4 are probably contained in an unpublished Master's dissertation by W. Carter—see [2, p. 706, footnote 11] —it seems desirable to consider them here, first, because of their form as quasigroup algebras, and secondly, because they are used in §16.) In §16 are given two distinct generalizations of the Cayley-Dickson division algebra of order 8, the second of which (Theorem 16C) is particularly broad. §17 considers the extension of a linear vector space, of order n over an arbitrary field, by the two-group, and studies those algebras which satisfy a certain condition common to the division algebras of Theorem 16C. We obtain in this way not only the algebras of Theorem 16C, but also some commutative division algebras of order $2n$ defined by L. E. Dickson. The work of this section, moreover, indicates an apparent limit to the usefulness of associative division algebras for defining non-associative division algebras.

It is perhaps only fair to warn the reader that we have used the terms "linear non-associative algebra" and "non-associative algebra" in the sense of "linear, not necessarily associative, algebra." However the adjective "non-associative," when used in other combinations, is to be given its ordinary meaning. Algebras are understood to have a finite basis over a field; otherwise we use the term ring.

2. **Simple algebras.** Let $\mathfrak{M}_n$ be a total matric algebra of degree n over an arbitrary field F. If $\mathfrak{S} \subset \mathfrak{M}_n$ is any set of linear transformations, we shall denote by $E(\mathfrak{S})$ the *enveloping algebra* of $\mathfrak{S}$ (in A. A. Albert's phraseology, the *polynomial algebra* generated by the transformations of $\mathfrak{S}$).

If $\mathfrak{A}$ is a linear non-associative algebra of order n over F, we may define two linear subsets of $\mathfrak{M}_n$, namely

$$\mathfrak{L} = (L_x), \qquad \mathfrak{R} = (R_x). \tag{2.1}$$

Here $\mathfrak{L}$, for example, consists of all transformations L_x defined by

$$xy = y^{L_x} = x^{R_y}, \tag{2.2}$$

where xy denotes the product of two arbitrary elements x, y of $\mathfrak{A}$. We now make two simple observations which are of importance for the sequel.

Since $\mathfrak{A}$ has order n, the linear sets $\mathfrak{L}$ and $\mathfrak{R}$ each have order n or less. More-

over if n transformations, linearly independent or not, be arbitrarily assigned in $\mathfrak{R}$ to correspond to a basis of $\mathfrak{A}$, then $\mathfrak{L}$ is uniquely determined (and conversely) since $\mathfrak{R}$ determines $\mathfrak{A}$ and $\mathfrak{A}$, $\mathfrak{L}$.

An algebra $\mathfrak{A}$ is here defined to be *right-simple* if and only if it contains no proper right ideals. *Left-simplicity* and *simplicity* are defined analogously. We do not exclude the case that $\mathfrak{A}$ is the zero algebra of order one.

THEOREM 2A. *$\mathfrak{A}$ is right-simple, left-simple, or simple if and only if $E(\mathfrak{R})$, $E(\mathfrak{L})$ or $E(\mathfrak{R}, \mathfrak{L})$ respectively are irreducible algebras.*

Proof. The part of this theorem which deals with simplicity has been proved by N. Jacobson [1, Corollary to Theorem 3, p. 546] and by A. A. Albert [2, Theorem 1, p. 693]. Although essentially the same proof will dispose of right-simplicity, we should like to give our own. First let us assume that $\mathfrak{A}$ has a right-ideal $\mathfrak{B}$ of order $m<n$, and let the basis e_i $(i=1, 2, \cdots, n)$ of $\mathfrak{A}$ be chosen so that e_α $(\alpha=1, 2, \cdots, m)$ is a basis of $\mathfrak{B}$. Since $e_\alpha \cdot x$ is in $\mathfrak{B}$ for every x of $\mathfrak{A}$, R_x has the representation

$$(2.3) \qquad R_x = \begin{pmatrix} U_x & 0 \\ * & * \end{pmatrix}, \qquad E(\mathfrak{R}) = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix},$$

and hence $E(\mathfrak{R})$ is a reducible algebra of transformations. Thus if $\mathfrak{A}$ is not right-simple, $E(\mathfrak{R})$ is reducible. Assume conversely that $E(\mathfrak{R})$ is reducible; then a basis of $\mathfrak{A}$ can be chosen so that $E(\mathfrak{R})$, and hence R_x, has the form given by (2.3), where U_x denotes a matrix of m rows and columns for some $m<n$. But then if e_α is any one of the first m basis elements of $\mathfrak{A}$, the subspace $\mathfrak{B}$ spanned by the e_α is a proper right-ideal of $\mathfrak{A}$, since $e_\alpha \cdot x$ is a linear combination of the e_α $(\alpha=1, 2, \cdots, m)$. Hence if $E(\mathfrak{R})$ is reducible, $\mathfrak{A}$ is not right-simple. It follows that $\mathfrak{A}$ is right-simple if and only if $E(\mathfrak{R})$ is irreducible.

If $\mathfrak{A}$ is the zero algebra of order one, $E(\mathfrak{L})$, $E(\mathfrak{R})$ and $E(\mathfrak{R}, \mathfrak{L})$ are irreducible algebras consisting of the zero transformation only. We leave aside this trivial case. If $\mathfrak{S}\neq 0$ is an irreducible sub-algebra of $\mathfrak{M}_n$ then, by the well known structure theorems of associative algebras, $\mathfrak{S}$ is the direct product of a total matric algebra and a division algebra, $\mathfrak{S}=\mathfrak{M}_p \times \mathfrak{D}$ where $\mathfrak{D}$ is a division algebra of order $d=n/p$ over F. A. A. Albert [2, Theorem 1, p. 693] shows that if $E(\mathfrak{R}, \mathfrak{L})=\mathfrak{M}_p \times \mathfrak{D}$ then $\mathfrak{D}$ is a field (that is, a commutative division algebra). That there is no corresponding restriction on $\mathfrak{D}$ in the case of right-simplicity is evidenced by the following theorem.

THEOREM 2B. *Let $\mathfrak{S}\neq 0$ be any irreducible sub-algebra of $\mathfrak{M}_n$. Then there exists a right-simple algebra $\mathfrak{A}$ of order n over F such that $E(\mathfrak{R})=\mathfrak{S}$.*

The proof of this theorem depends upon the first sentence of the following lemma.

LEMMA 2A. *There exist two transformations P and Q of $\mathfrak{M}_n$ such that*

$E(P, Q) = \mathfrak{M}_n$. One, both, or neither of P and Q may be taken to be nonsingular.

We shall assume the truth of the lemma for the moment, and proceed with the proof of Theorem 2B. Let $\mathfrak{S} = \mathfrak{M}_p \times \mathfrak{D}$ as before, where $\mathfrak{D}$ has order $d = n/p$. Then if e_i $(i = 1, 2, \cdots, n)$ is a basis of $\mathfrak{A}$ we wish to pick the n transformations $R_i = R_{e_i}$ so that $E(\mathfrak{R}) \equiv E(R_1, R_2, \cdots, R_n) = \mathfrak{S}$. We may ignore the trivial case $n = 1$, and assume $n \geqq 2$. If $p = n$, so that $d = 1$, $\mathfrak{D} = F$, we may set $R_1 = P$, $R_2 = Q$, and assign the other R_i arbitrarily; then $E(\mathfrak{R}) = \mathfrak{M}_n$ by Lemma 2A. If $p = 1$ we may pick the R_i to be a basis of $\mathfrak{D}$, and obtain $E(\mathfrak{R}) = \mathfrak{D}$. Finally if $1 < p < n$ (so that $p \geqq 2$ and $n = dp \geqq 4$) we have $d + 2 = (n/p) + 2 \leqq (n/2) + (n/2) = n$. In this case, if I_p and I_d are respectively the units of $\mathfrak{M}_p$ and $\mathfrak{D}$, we may choose R_1, R_2 so that $E(R_1, R_2) = \mathfrak{M}_p \times I_d$ and pick d of the remaining R_i to form a basis of $I_p \times \mathfrak{D}$. In whatever manner the remaining $n - d - 2$ of the R_i be chosen, it is clear that $E(\mathfrak{R}) \supset \mathfrak{M}_p \times \mathfrak{D}$; and in fact we shall have $E(\mathfrak{R}) = \mathfrak{M}_p \times \mathfrak{D}$ if and only if these remaining R_i be chosen in $\mathfrak{M}_p \times \mathfrak{D}$.

Theorem 2B suggests the unsolved problem of determining all right-simple algebras $\mathfrak{A}$ such that $E(\mathfrak{R}) = \mathfrak{S}$ for a fixed irreducible algebra $\mathfrak{S}$. This would appear to involve the study of all possible sets of r generators of $\mathfrak{S}$, for $1 \leqq r \leqq n$, where we assume that no $r - 1$ of a given set of r generators will generate $\mathfrak{S}$.

We now proceed to a proof of Lemma 2A. As B. Vinograde has pointed out, the following approach is valid for transformations over an arbitrary associative ring with a unit element. (Note in addition that for the proof of the first statement of Lemma 2A we make no use of the associative law of multiplication.) A proof of a somewhat stronger lemma, for the case of transformations over a field, may be found in a well known textbook by A. A. Albert [5, p. 95, Exercise 3].

Proof of Lemma 2A. Let the transformations e_{ij} $(i, j = 1, 2, \cdots, n)$ form the familiar linear basis of $\mathfrak{M}_n$, so that the product $e_{ij}e_{pq}$ is e_{iq} or 0 according as $j = p$ or $j \neq p$. Define the singular transformations

$$\begin{aligned} P &= F_n = e_{12} + e_{23} + \cdots + e_{n-1,n}, \\ Q &= G_n = e_{21} + e_{32} + \cdots + e_{n,n-1}, \end{aligned} \tag{2.4}$$

and denote $E(F_n, G_n)$ by $\mathfrak{E}_n$. Since the proof proceeds by induction, let $n = 2$ in (2.1), whence $F_2 = e_{12}$, $G_2 = e_{21}$. Then $\mathfrak{E}_2$ contains the linear basis of $\mathfrak{M}_2$, namely $F_2G_2 = e_{11}$, $F_2 = e_{12}$, $G_2 = e_{21}$, $G_2F_2 = e_{22}$; and hence $\mathfrak{E}_2 = \mathfrak{M}_2$. Now assume that $\mathfrak{E}_{n-1} = \mathfrak{M}_{n-1}$ for some $n > 2$. By successive multiplication we find that $\mathfrak{E}_n$ contains the elements

$$\begin{aligned} F_nG_n &= e_{11} + e_{22} + \cdots + e_{n-1,n-1}, \\ G_nF_n &= e_{22} + \cdots + e_{n-1,n-1} + e_{nn}, \\ F_nG_n \cdot G_nF_n &= e_{22} + \cdots + e_{n-1,n-1}, \end{aligned}$$

and $G_nF_n - F_nG_n \cdot G_nF_n = e_{nn}$. Hence $\mathfrak{E}_n$ contains $F_ne_{nn} = e_{n-1,n}$, $e_{nn}G_n = e_{n,n-1}$, $F_n - e_{n-1,n} = F_{n-1}$, $G_n - e_{n,n-1} = G_{n-1}$. To sum up, $\mathfrak{E}_n$ contains e_{nn}, $e_{n,n-1}$, $e_{n-1,n}$ and $E(F_{n-1}, G_{n-1}) \equiv \mathfrak{E}_{n-1} = \mathfrak{M}_{n-1}$. Since e_{ij} is in $\mathfrak{M}_{n-1}$ for $i, j < n$, we have that $\mathfrak{E}_n$ also contains $e_{n,n-1}e_{n-1,i} = e_{ni}$ and $e_{i,n-1}e_{n-1,n} = e_{in}$ for $i < n$. Thus finally $\mathfrak{E}_n = \mathfrak{M}_n$.

If I_n is the n-dimensional identity transformation and F_n is defined by (2.4), then $C = I_n + F_n$ is nonsingular, and $E(C)$ contains I_n and hence $C - I_n = F_n$. This remark should suffice to show the truth of the following statement, with which the proof of Lemma 2A is completed.

$$(2.5) \qquad E(I_n + F_n, G_n) = E(I_n + F_n, I_n + G_n) = E(F_n, G_n) = \mathfrak{M}_n,$$

where F_n, G_n are given by (2.4).

The following lemma is well known.

Lemma 2B. *If $\mathfrak{S} \subset \mathfrak{M}_n$ is an irreducible subalgebra of an algebra $\mathfrak{T} \subset \mathfrak{M}_n$, then $\mathfrak{T}$ is also irreducible.*

Proof. The reducibility of $\mathfrak{T}$ would force that of $\mathfrak{S}$.

Theorem 2C. *Let $\mathfrak{A}$ be a linear algebra of order n over a field F. Assume that $\mathfrak{A}$ has a unity quantity e but is otherwise arbitrary. Then*

(i) *regardless of the nature of F, there exists an isotope $\mathfrak{A}_o$ of $\mathfrak{A}$ which is simple;*

(ii) *if F possesses an extension field $F(\theta)$ of degree n, there exists an isotope $\mathfrak{A}_o$ of $\mathfrak{A}$ which is not only simple but right-simple and left-simple.*

Theorem 2D. *Let $\mathfrak{A}$ be a linear algebra of order n over a field F which possesses an extension field $F(\theta)$ of degree n. Let $\mathfrak{A}$ have a right-unit e but be otherwise arbitrary (so that, for example, every element of $\mathfrak{A}$ may be left-singular). Then there exists an isotope $\mathfrak{A}_o$ of $\mathfrak{A}$ which is right-simple.*

These theorems demonstrate the non-invariance under general isotopic transformations of the property of simplicity, and prepare us for the idea of *isotopic simplicity* which will be introduced in the next section. Part (ii) of Theorem 2C has been given by Albert [2, Theorem 11, p. 699] but the other results seem to be new.

Proof of Theorem 2C and 2D. Let $\mathfrak{A}_o$ be a principal isotope of $\mathfrak{A}$, defined by

$$(2.6) \qquad xoy = x^P \cdot y^Q,$$

where P, Q are nonsingular transformations to be determined. First take the case that $\mathfrak{A}$ has a unit element e. We may set $u = e^{P^{-1}}$, $v = e^{Q^{-1}}$ and find

$$\overset{o}{L}_u = Q, \qquad \overset{o}{R}_v = P.$$

If P, Q are chosen, by authority of Lemma 2A, so that $E(P, Q) = \mathfrak{M}_n$, we have

$E(\mathfrak{R}_o)=\mathfrak{M}_n$; $\mathfrak{A}_o$ is (central) simple. On the other hand, if F possesses an extension field $K=F(\theta)$ of degree n, we may choose P to be a generator of a field isomorphic to K. In this case $E(P)$ is irreducible, $E(\mathfrak{R}_o)\supset E(P)$, $E(\mathfrak{R}_o)$ is irreducible, $\mathfrak{A}_o$ is right-simple. If a like choice be made for Q, then $\mathfrak{A}_o$ is left-simple as well. Finally, under the hypotheses of Theorem 2D we still have $R_v^o=P$, and we may choose P as above so that $\mathfrak{A}_o$ is right-simple.

We note in passing that *if* $\mathfrak{A}$, *of order* $n\geqq 3$, *is any algebra with a unit element e, we may use equation* (2.6) *to define a simple algebra* $\mathfrak{A}_o$, *not isotopic to* $\mathfrak{A}$, *in which every element is a right-hand and left-hand divisor of zero.* For example, let $P=T^{-1}F_nT$, $Q=T^{-1}G_nT$, where F_n, G_n are the matrices (2.4) and T is a nonsingular matrix such that $e_2^T=e_1=e$. (Here $e_1=e$, $e_2, \cdots, e_n$ is a basis of $\mathfrak{A}$.) Then if $u=e_1^T$, $v=e_3^T$, we have $u^P=e$, $v^Q=e$ and hence $L_u^o=Q$, $R_v^o=P$. It follows that $E(P, Q)=T^{-1}E(F_n, G_n)T=\mathfrak{M}_n$, that $\mathfrak{A}_o$ is simple, and that every element of $\mathfrak{A}_o$ is a two-sided zero-divisor.

3. **Isotopically simple algebras.** An algebra $\mathfrak{A}$ is said to be *isotopically simple* if every isotope of $\mathfrak{A}$ (and hence of course $\mathfrak{A}$ itself) is simple. Similar meanings are given to the terms *isotopically right-simple* and *isotopically left-simple.* In view of Theorems 2A, 2B, the following theorems show the existence of such algebras.

THEOREM 3A. *If a right-simple algebra has a right-unit, then it is isotopically right-simple.*

THEOREM 3B. *If a simple algebra has a unit element, then it is isotopically simple.*

It follows from Theorem 3B in particular that every simple associative algebra is isotopically simple.

Proof of the theorems. Let $\mathfrak{A}_o$ be a principal isotope of an algebra $\mathfrak{A}$, so that

$$xoy = x^P\cdot y^Q$$

for nonsingular transformations P and Q. Then

$$\overset{o}{L_x} = QL_{x^P}, \qquad \overset{o}{R_y} = PR_{y^Q}.$$

If $\mathfrak{A}$ has a right-unit e then $E(\mathfrak{R}_o)$ contains P and hence contains $P^{-1}\subset E(P)$. Thus $E(\mathfrak{R}_o)\supset P^{-1}R_y^o$ for every y, $E(\mathfrak{R}_o)\supset E(\mathfrak{R})$, $E(\mathfrak{R}_o)=E(P, \mathfrak{R})$. It follows from Lemma 2B and Theorem 2A that $\mathfrak{A}_o$ is right-simple when $\mathfrak{A}$ is. Similarly, if e is a two-sided unit of $\mathfrak{A}$, we have $E(\mathfrak{R}_o)=E(P, \mathfrak{R})$, $E(\mathfrak{L}_o)=E(Q, \mathfrak{L})$, and $E(\mathfrak{R}_o, \mathfrak{L}_o)=E(P, Q, \mathfrak{R}, \mathfrak{L})$. Hence if $\mathfrak{A}$ is simple it follows that $\mathfrak{A}_o$ is simple too. Since every isotope of $\mathfrak{A}$ is isomorphic to a principal isotope the proof is complete.

Every non-associative algebra may be built up from isotopically simple algebras, as our next theorem shows.

THEOREM 3C. *Every algebra $\mathfrak{A}$ of order n possesses an isotope $\mathfrak{B}$ with a decomposition series*

$$\mathfrak{B} = \mathfrak{B}_0 \supset \mathfrak{B}_1 \supset \mathfrak{B}_2 \supset \cdots \supset \mathfrak{B}_k = (0) \tag{3.1}$$

in which the difference algebras $\mathfrak{C}_i \equiv \mathfrak{B}_{i-1} - \mathfrak{B}_i$ $(i=1, 2, \cdots, k)$ are isotopically simple. The problem of constructing the most general algebra $\mathfrak{B}$ with a given set of difference algebras $\mathfrak{C}_i$ $(i=1, 2, \cdots, k)$ is trivial.

Proof. If $\mathfrak{A}$ is isotopically simple we have nothing to prove. Hence assume that $\mathfrak{A}$ has an isotope, which we may as well take to be $\mathfrak{A}$ itself, with a proper ideal $\mathfrak{A}_1$ of order m, $0<m<n$. If we pick $e_1, e_2, \cdots, e_m$ to be a basis of $\mathfrak{A}_1$ and let $e_{m+1}, \cdots, e_n$ complete the basis of $\mathfrak{A}$, every element of $\mathfrak{A}$ has, relative to this basis, the unique decomposition

$$x = x_1 + x_2 \tag{3.2}$$

where x_1 is in $\mathfrak{A}_1$ and x_2 is in the linear set spanned by $e_{m+1}, \cdots, e_n$. The elements x_2, under the multiplication of $\mathfrak{A}$ taken modulo $\mathfrak{A}_1$, form a difference algebra $\mathfrak{A}_2 \equiv \mathfrak{A} - \mathfrak{A}_1$. If $\mathfrak{A}_2$ is isotopically simple we turn our attention to $\mathfrak{A}_1$. But if the contrary is the case, we may define arbitrary nonsingular linear transformations U_2, V_2 of the linear set $\mathfrak{A}_2$, set

$$x^{U} = x_1 + x_2^{U_2}, \qquad y^{V} = y_1 + y_2^{V_2}, \tag{3.3}$$

and define a principal isotope $\mathfrak{A}^o$ of $\mathfrak{A}$ by

$$xoy = x^U \cdot y^V. \tag{3.4}$$

It is clear from (3.3) and (3.4) that $\mathfrak{A}_1$ is a proper ideal of $\mathfrak{A}^o$, and that

$$x_2 o y_2 \equiv x_2^{U_2} \cdot y_2^{V_2} \qquad (\text{modulo } \mathfrak{A}_1). \tag{3.5}$$

Thus we obtain a difference algebra $\mathfrak{A}_2^o \equiv \mathfrak{A}^o - \mathfrak{A}_1$ of $\mathfrak{A}^o$ which is an arbitrary principal isotope of $\mathfrak{A}_2 = \mathfrak{A} - \mathfrak{A}_1$. Since $\mathfrak{A}_2$ is not isotopically simple, there exists an $\mathfrak{A}_2^o$ which has a proper ideal, say of order n_1, and, correspondingly, $\mathfrak{A}^o$ has a proper ideal of order $m_1 = m + n_1$ containing $\mathfrak{A}_1$. We then replace $\mathfrak{A}_1$ by the larger proper ideal and investigate the smaller difference algebra. After a finite number of such steps we must arrive at a difference algebra $\mathfrak{C}_1$ which is isotopically simple.

We have thus proven that some isotope of $\mathfrak{A}$ has a proper ideal such that the corresponding difference algebra is isotopically simple. For convenience, assume that this is $\mathfrak{A}$ itself, the proper ideal being $\mathfrak{A}_1$. Making an induction on the order of our algebras, we assume that Theorem 3B holds for all algebras of order less than n, and hence for $\mathfrak{A}_1$. Then $\mathfrak{A}_1$ has an isotope $\mathfrak{B}_1$, which we may assume to be a principal isotope, with a decomposition series

$$\mathfrak{B}_1 \supset \mathfrak{B}_2 \supset \cdots \supset \mathfrak{B}_k$$

such that the difference algebras $\mathfrak{C}_i \equiv \mathfrak{B}_{i-1} - \mathfrak{B}_i$ ($i = 2, 3, \cdots, k$) are isotopically simple. If $\mathfrak{B}_1$ is obtained from $\mathfrak{A}_1$ by

$$x_1 o y_1 = x_1^{U_1} \cdot y_1^{V_1}, \tag{3.6}$$

we set

$$x^U = x_1^{U_1} + x_2, \qquad y^U = y_1^{V_1} + y_2 \tag{3.7}$$

and define $\mathfrak{B} = \mathfrak{A}_o$ by

$$x o y = x^U \cdot y^V. \tag{3.8}$$

Since $\mathfrak{A}_1$ and $\mathfrak{B}_1$ consist of the same elements, it follows from (3.7) and (3.8) that $\mathfrak{C}_1 \equiv \mathfrak{A} - \mathfrak{A}_1 = \mathfrak{B} - \mathfrak{B}_1$.

This completes the proof of the first part of Theorem 3C. It is still an open question as to whether the number k is the same for all isotopes $\mathfrak{B}$ with the stated type of decomposition series; and if this should be the case it would be interesting to know whether the difference algebras $\mathfrak{C}_i$ are uniquely determined (except possibly for order) in the sense of isotopy. As to the second part of the theorem, it is sufficient to consider the case of an algebra $\mathfrak{A}$ with a proper ideal $\mathfrak{A}_1$. Let i, j, k have the range $1, 2, \cdots, m$, let p, q, r have the range $m+1, \cdots, n$, let the e_i form a basis of $\mathfrak{A}_1$, and let the e_p complete the basis of $\mathfrak{A}$. Then multiplication in $\mathfrak{A}_1$ is completely described by

$$e_i e_j = \sum c_{ijk} e_k, \tag{3.9}$$

where the c_{ijk} are constants, while multiplication in $\mathfrak{A}$ is determined by (3.9) and

$$\begin{aligned} e_p e_j &= \sum c_{pjk} e_k + \sum c_{pjr} e_r, \\ e_i e_q &= \sum c_{iqk} e_k + \sum c_{iqr} e_r, \\ e_p e_q &= \sum c_{pqk} e_k + \sum c_{pqr} e_r. \end{aligned} \tag{3.10}$$

Finally, multiplication in the difference algebra $\mathfrak{A}_o = \mathfrak{A} - \mathfrak{A}_1$ is given by

$$e_p o e_q = \sum c_{pqr} e_r. \tag{3.11}$$

Thus if the basis in $\mathfrak{A}$ is adapted to $\mathfrak{A}_1$ (to use H. Weyl's phrase) the constants c_{ijk} and c_{pqr} completely determine $\mathfrak{A}_1$ and $\mathfrak{A}_o$, and conversely. Given $\mathfrak{A}_1$ and $\mathfrak{A}_o$, the most general $\mathfrak{A}$ with proper ideal $\mathfrak{A}_1$ and difference algebra $\mathfrak{A}_o$ is clearly isomorphic to an algebra defined by (3.9) and (3.10), where the constants c_{pjk}, c_{pjr}, c_{iqk}, c_{iqr}, and c_{pqk} are arbitrarily assigned.

Our next concern is the problem of the construction of isotopically simple algebras. The only such algebras of order one are the field F itself and the zero algebra of order one. However, in preparation for a closer study of isotopically simple algebras, we find it convenient to consider some other matters first.

Following Albert [2, p. 690] we define an element x of an algebra $\mathfrak{A}$ to be *right singular* or *right nonsingular* according as the corresponding right multiplication R_x is singular or nonsingular. *Left singularity* and *left nonsingularity* are to be defined analogously. We state without proof the following theorem.

THEOREM 3D. (i) *An algebra $\mathfrak{A}$ has an isotope with a right-unit element if and only if $\mathfrak{A}$ possesses a right nonsingular element.*

(ii) *$\mathfrak{A}$ has an isotope with a (two-sided) unit element if and only if $\mathfrak{A}$ possesses at least one right nonsingular element and one left nonsingular element.*

Part (ii) of the theorem has been given by Albert [2, Theorem 7, p. 698] and the proof of Part (i) is readily deduced from that of Part (ii).

It is evident that algebras may be divided under isotopy into four classes, as follows:

(I) *All algebras with at least one right nonsingular and one left nonsingular element.* Such an algebra $\mathfrak{A}$ has an isotope $\mathfrak{A}_o$ with a unit element, and $\mathfrak{A}$ is isotopically simple if and only if $\mathfrak{A}_o$ is simple.

(II) *All algebras with at least one right nonsingular element but with no left nonsingular element.* Such an $\mathfrak{A}$ has an isotope $\mathfrak{A}_o$ with a right-unit (but none with a two-sided unit) and is isotopically right-simple if and only if $\mathfrak{A}_o$ is right-simple.

(III) *The class similar to* (II) *but with the roles of "right" and "left" interchanged.*

(IV) *All algebras with no right or left nonsingular elements.*

Under class (I) come in particular the *division algebras*, that is, those algebras in which every element is both right and left nonsingular. Such an algebra clearly possesses no right or left ideals, and since every isotope of a division algebra is obviously a division algebra, we have that every division algebra is isotopically right-simple and left-simple.

THEOREM 3E. *If an algebra $\mathfrak{A}$ of order two over a field F is isotopically simple, then $\mathfrak{A}$ is isotopic to a field of degree two over F.* (*Hence such algebras do not exist for arbitrary F.*)

COROLLARY. *Every division algebra of order two is isotopic to a field.*

Proof. If $\mathfrak{A}$ belongs to class (I) we may assume that $\mathfrak{A}$ has a unit element e. If f is the other basis element then

$$ee = e, \qquad ef = fe = f, \qquad ff = \alpha e + \beta f.$$

It is easily seen that $\mathfrak{A}$ is both commutative and associative, and since $\mathfrak{A}$ is also simple and of prime order it must be a field. If $\mathfrak{A}$ belongs to class (II) we assume that it has a right-unit e. Since e is left-singular but $ee=e$, it must be possible to choose a basis element f such that $ef=0$. In particular, (e) is a right ideal. If $ff=\alpha e+\beta f$, define $\mathfrak{A}_o$ by $xoy=x\cdot y^T$ where $e^T=\beta e-f$, $f^T=f$. Then (e) is still a right ideal; but it is in fact a two-sided ideal, since $foe=\beta f-(\alpha e+\beta f)=-\alpha e$. The case that $\mathfrak{A}$ is in class (III) is similarly disposed of. If $\mathfrak{A}$ is in class (IV) there must exist two elements e, a such that $ea\neq 0$, else $\mathfrak{A}$ would be the (non-simple) zero algebra of order two. We may define $\mathfrak{A}_o$ by $xoy=(x\cdot y^S)^T$ with $e^S=a$, $(ea)^T=e$, and have $eoe=e$. If f is the other basis element, eof and foe must lie in (e), since e is left and right singular; and thus $\mathfrak{A}_o$ has a proper ideal.

THEOREM 3F. *Let F be an arbitrary underlying field. Then* (i) *there exist isotopically simple algebras of class* (I), *order n, for every integer $n\geqq 3$*; (ii) *there exist isotopically right-simple algebras of class* (II), *order n, for every integer $n\geqq 4$.*

Proof by example. (i) Consider the commutative algebra $\mathfrak{A}=(e, e_i; i=1, 2, \cdots, n-1; n\geqq 3)$, where e is the unit element and $e_ie_i=e$, $e_ie_j=0$ for $i\neq j$. If $x=\alpha e+\sum\alpha_ie_i$ and i, j are distinct we have $(xe_i\cdot e_j)e_j=\alpha_ie$. Thus if α_i is different from zero for some i, the ideal generated by x contains e and hence $\mathfrak{A}$. Therefore $\mathfrak{A}$ is simple, and $\mathfrak{A}$ is isotopically simple by Theorem 3B. (Because of commutativity, $\mathfrak{A}$ is in fact isotopically right-simple and left-simple.)

(ii) Assuming $n\geqq 4$, define $R_{e_1}=I$, $R_{e_2}=P$, $R_{e_3}=Q$, $R_{e_i}=0$ for $i>3$, where P, Q are chosen so that $E(P, Q)=\mathfrak{M}_n$. Then if $\mathfrak{A}=(e_i; i=1, 2, \cdots, n; n\geqq 4)$ we see that $\mathfrak{A}$ has right-unit e_1, that $e_je_4=0$ for $j=1, 2, \cdots, n$, and that $\mathfrak{A}$ is right-simple. It follows from Theorem 3A that $\mathfrak{A}$ is isotopically right-simple of class (II).

THEOREM 3G. *If there exists a field of degree* 3 *over the underlying field F, then there exists an isotopically right-simple algebra of class* (II), *order* 3.

Proof. We need merely take $R_{e_1}=I$, $R_{e_2}=P$, $R_{e_3}=0$, where P generates a field of degree 3 over F.

We have omitted mention of algebras of class (III), since these algebras are anti-isomorphic to the algebras of class (II). The algebras of class (IV) present considerable difficulty, and will be studied from another point of view in §4.

The simple algebras of class (IV), order $n\geqq 3$, which were constructed in the last paragraph of the preceding section, are not isotopically simple.

4. **Trilinear forms.** With every linear non-associative algebra $\mathfrak{A}$ of order n there may be associated a trilinear form $F(x, y, z)$ in three n-dimensional vectors x, y, z, where $x=(x_1, x_2, \cdots, x_n)$. If e_i $(i=1, 2, \cdots, n)$ is a basis of $\mathfrak{A}$, we have

$$(4.1)\qquad e_ie_j=\sum c_{ijk}e_k$$

for some set of n^3 constants c_{ijk}. The corresponding trilinear form is

$$F(x, y, z) = \sum_{i,j,k} c_{ijk}x_iy_jz_k. \tag{4.2}$$

From (4.1) we see that if

$$x = \sum x_ie_i, \qquad y = \sum y_je_j \tag{4.3}$$

then

$$xy = \sum c_{ijk}x_iy_je_k. \tag{4.4}$$

Hence if $\mathbf{e}$ designates the symbolic vector $(e_1, e_2, \cdots, e_n)$ we have from (4.2) and (4.3) the equation

$$xy = F(x, y, \mathbf{e}). \tag{4.5}$$

Stepping aside for a few paragraphs from the main subject of this section, we note that, corresponding to a given trilinear form $F(x, y, z)$, we may define six linear algebras by taking the product of x and y to be $F(x, y, \mathbf{e})$, $F(y, x, \mathbf{e})$, $F(x, \mathbf{e}, y)$, $F(y, \mathbf{e}, x)$, $F(\mathbf{e}, x, y)$, or $F(\mathbf{e}, y, x)$. We shall speak of these six algebras as *associated.* The following theorem does not seem to be in the literature, although it is probably well known.

THEOREM 4A. *If $\mathfrak{A}$ is a division algebra then each of the other five algebras associated with $\mathfrak{A}$ is also a division algebra.*

In the general case that $\mathfrak{A}$ is a non-associative ring we say that left division is always possible in $\mathfrak{A}$ if for every z and for every nonzero x of $\mathfrak{A}$ the equation $xy=z$ is uniquely solvable for y in $\mathfrak{A}$. It should be clear what is meant by the statement that right division is always possible in $\mathfrak{A}$. Then $\mathfrak{A}$ is by definition a division ring if and only if both left and right division are always possible in $\mathfrak{A}$. If, as in the present case, $\mathfrak{A}$ is a linear algebra of finite order over a field, we call $\mathfrak{A}$ a division algebra. It will appear in our proof that $\mathfrak{A}$ is a division algebra if and only if it has no divisors of zero, that is, if the equation $xy=0$ is impossible unless at least one of x and y is zero. That the corresponding statement is false for rings is evident from the familiar example of the ring consisting of zero and the positive and negative integers under ordinary addition and multiplication.

Proof of Theorem 4A. Since $xy=x^{L_y}=y^{R_x}$, a linear algebra is a division algebra if and only if both L_x and R_x are nonsingular transformations for every nonzero x, or if the determinants $|L_x|$, $|R_x|$ are nonzero for every nonzero x. But if multiplication is given in $\mathfrak{A}$ by (4.4) or (4.5), then L_x and R_x are the first two of the following matrices:

$$L_x = (\sum c_{kij}x_k), \qquad R_x = (\sum c_{ikj}x_k), \qquad M_x = (\sum c_{ijk}x_k). \tag{4.6}$$

Here i, j are respectively the row and column indices, and k is to be summed from 1 to n. Again, if $\overline{\mathfrak{A}}$ is an algebra associated with $\mathfrak{A}$, with multiplication given for example by $(x, y)=F(x, e, y)$, we find $\bar{L}_x=L_x'$ and $\bar{R}_x=M_x$, where U' is the transpose of the matrix U. Similarly, the right and left multiplications of each associate of $\mathfrak{A}$ are among the six matrices consisting of L_x, R_x, M_x and their transposes. Hence we shall really prove the following.

LEMMA 4A. *If any one of the three determinants*

$$(4.7)\qquad \left|\sum c_{kij}x_k\right|, \qquad \left|\sum c_{ikj}x_k\right|, \qquad \left|\sum c_{ijk}x_k\right|$$

is different from zero for all nonzero vectors $x=(x_1, x_2, \cdots, x_n)$ then the same is true of the other two[2].

Indeed if L_x is nonsingular for every $x\neq 0$ the equation $xy=0$, $x\neq 0$, implies $y=0$. Hence x^{R_y} is nonzero for all nonzero x and y. It follows that R_y is nonsingular for all $y\neq 0$. Since the converse is clearly true we have that if one of $|L_x|$, $|R_x|$ is not equal to 0 for all $x\neq 0$ then so is the other. But, assuming $|L_x|\neq 0$ for $x\neq 0$, we refer to the algebra $\bar{\mathfrak{A}}$ defined above and find $|\bar{L}_x|=|L_x'|=|L_x|\neq 0$, whence $|\bar{R}_x|=|\mathrm{M}_x|$ is not equal to 0, for all $x\neq 0$. The above lemma allows us considerable choice in the matter of proving that an algebra is a division algebra.

Returning to the algebra $\mathfrak{A}$ defined by (4.4) or (4.5), let us consider the isotope $\mathfrak{A}_o$ of $\mathfrak{A}$ with multiplication given by

$$(4.8)\qquad xoy = (x^U\cdot y^V)^W.$$

Then a reference to (4.4) and (4.5) shows that

$$(4.9)\qquad xoy = F(x^U, y^V, e^{W'}),$$

where W' is the transpose of W. Thus the trilinear form associated with $\mathfrak{A}_o$ is $G(x, y, z)=F(x^U, y^V, z^{W'})$. We may call two such forms *isotopic*, and speak of either one as being the *isotope* of the other. We note that the six algebras associated with G are respectively isotopic (in slightly different ways) to the six algebras associated with F.

It should be evident from the preceding remarks that the theory of nonassociative algebras under isotopy can be put into one-to-one correspondence with the theory of trilinear forms in three digredient n-dimensional vectors. (In connection with the latter, see for example [7], in which will also be found an extensive bibliography.) At the present time however the two theories have little in common; they have not been concerned with the same problems. In the rest of this section we shall consider the theory of isotopically simple algebras from the standpoint of trilinear forms.

Let us suppose that $\mathfrak{A}_o$, given by (4.8), has a right-ideal of order $r<n$ spanned by the first r basis elements $e_1, e_2, \cdots, e_r$. Then if $p=x^V$,

[2] In another notation, L. E. Dickson [6, p. 370] proved that if $|R_x|$ is nonzero for every nonzero x the same is true of $|L_x|$, and conversely. Dickson seems to have abandoned this result shortly afterwards, as far as the author can judge from his later writings.

$$(4.10)\qquad \overset{o}{R}_x = UR_pW = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix},$$

where the block of zeros in the matrix on the right has r rows and $n-r$ columns. It follows that if $u=(u_1, u_2, \cdots, u_n)$ is any one of the first r rows of U and $w=(w_1, w_2, \cdots, w_n)$ is the transpose of any one of the last $n-r$ columns of W we have $u\cdot R_p\cdot w'=0$ for all p, or, in view of (4.6),

$$\sum_{i,k,j} c_{ikj}u_i p_k w_j = 0$$

for all p_k. If we equate the coefficient of each p_k to zero the result may be written in any one of the following forms:

$$(4.11)\qquad L_u\cdot w' = 0 \quad \text{or} \quad u\cdot M_w = 0 \quad \text{or} \quad F(u, e, w) = 0.$$

Hence we have essentially proved Part (i) of the following theorem.

THEOREM 4B. (i) *A necessary and sufficient condition that an algebra* $\mathfrak{A}$ *of order* n *should possess an isotope with a right ideal of order* r *is that there exist linear sets* $\mathfrak{U}$ *and* $\mathfrak{W}$, *of orders* r *and* $n-r$ *respectively, consisting of* n*-dimensional row vectors, such that any one of the* (*equivalent*) *equations* (4.11) *holds for every* u *of* $\mathfrak{U}$ *and* w *of* $\mathfrak{W}$.

(ii) *A necessary and sufficient condition that an algebra* $\mathfrak{A}$ *of order* n *should possess an isotope with a left ideal of order* r *is that there exist linear sets* $\mathfrak{V}$ *and* $\mathfrak{W}$, *of orders* r *and* $n-r$ *respectively, consisting of* n*-dimensional row vectors, such that any one of the* (*equivalent*) *equations* (4.12) *below holds for every* v *of* $\mathfrak{V}$ *and* w *of* $\mathfrak{W}$.

$$(4.12)\qquad R_v\cdot w' = 0 \quad \text{or} \quad v\cdot M'_w = 0 \quad \text{or} \quad F(e, v, w) = 0.$$

(iii) *A necessary and sufficient condition that an algebra* $\mathfrak{A}$ *of order* n *should possess an isotope with a two-sided ideal of order* r *is that there exist linear sets* $\mathfrak{U}$, $\mathfrak{V}$, *and* $\mathfrak{W}$, *of orders* r, r, *and* $n-r$ *respectively, consisting of* n*-dimensional row vectors, such that the equations* (4.11) *and* (4.12) *hold simultaneously for every* u *of* $\mathfrak{U}$, v *of* $\mathfrak{V}$, *and* w *of* $\mathfrak{W}$.

The reader should have no difficulty in completing the proof of Theorem 4B. Note for future reference that *the sums of the orders of* $\mathfrak{U}$ *and* $\mathfrak{W}$ ($\mathfrak{V}$ *and* $\mathfrak{W}$) *is* n. It may be seen moreover that if the word "isotope" be replaced by "isomorph" in part (iii) of the theorem, for example, the only additional conditions are that $\mathfrak{U}=\mathfrak{V}$ and that $u\cdot w'=0$ for every u of $\mathfrak{U}$ and w of $\mathfrak{W}$.

Since we have found it possible in §3 to handle problems of isotopic simplicity by other methods for algebras of classes I, II and III, we shall now direct attention to algebras of class IV. It follows that to every $x\neq 0$ of $\mathfrak{A}$ there corresponds at least one $y\neq 0$ (and to every y at least one x), such that $xy=0$. As a special case we may consider the *anti-commutative* algebras, those which obey the laws

$$x^2 = 0, \qquad xy + yx = 0. \tag{4.13}$$

(Note that if the underlying field has characteristic different from two, either of these laws implies the other.) The equations (4.13), in terms of the form $F(x, y, z)$, become

$$c_{iik} = 0, \qquad c_{ijk} + c_{jik} = 0. \tag{4.14}$$

Reference to Theorem 4B shows the truth of the following.

THEOREM 4C. *If $\mathfrak{A}$ is an anti-commutative algebra, then $\mathfrak{A}$ is isotopically simple if and only if it is isotopically right simple and left simple.*

In fact if (4.11) is satisfied, so that an isotope of $\mathfrak{A}$ has a right ideal, (4.12) is also satisfied with the same $\mathfrak{W}$ and with $\mathfrak{V} = \mathfrak{U}$. Thus the property of being anti-commutative, although it is readily seen not to prevail under isotopy, does allow a worthwhile simplification of the theory of isotopic simplicity. A like remark would hold true for commutative algebras, but these however are not in general of class IV.

We shall speak of an algebra $\mathfrak{A}$ as being *totally skew-symmetric* if the coefficients of the trilinear form $F(x, y, z)$ are totally skew-symmetric, that is, if c_{ijk} vanishes whenever two of the indices i, j, k are equal and changes sign when any two indices are interchanged. In particular, a totally skew-symmetric algebra is anti-commutative, but not conversely. Moreover the property of being totally skew-symmetric, like that of being anti-commutative, is not an isotopic invariant. For a totally skew-symmetric algebra the equation $F(u, \mathbf{e}, w) = 0$ implies $F(u, w, \mathbf{e}) = 0$. Thus from Theorems 4B, 4C we obtain the following theorem.

THEOREM 4D. *Let $\mathfrak{A}$ be a totally skew-symmetric algebra. Then*

(i) *a necessary and sufficient condition that $\mathfrak{A}$ possess an isotope with a right, left, or two-sided ideal of order r is that there exist a linear subset $\mathfrak{X}$ of $\mathfrak{A}$ of order r and a linear subset $\mathfrak{Y}$ of $\mathfrak{A}$ of order $n - r$ such that $xy = 0$ for every x of $\mathfrak{X}$ and y of $\mathfrak{Y}$;*

(ii) *if $\mathfrak{A}$ has an isotope with an ideal of order r then $\mathfrak{A}$ has an isotope with an ideal of order $n - r$.*

COROLLARY 1. *If $\mathfrak{A}$ is merely isotopic to a totally skew-symmetric algebra, the statements of Theorem 4D still hold true.*

COROLLARY 2. *The simple Lie algebra of order 3, consisting of the ordinary three-dimensional vectors under the outer (or cross) product, is isotopically right-simple and left-simple.*

Proof. A comparison of Part (ii) of Theorem 4D with Theorem 4B shows that we have simply replaced $\mathfrak{U}$ (or $\mathfrak{V}$) by $\mathfrak{X}$ and $\mathfrak{W}$ by $\mathfrak{Y}$. Part (ii) follows since we may interchange the roles of $\mathfrak{X}$ and $\mathfrak{Y}$, if these sets exist, in view of the fact that $xy=-yx$. As for Corollary 1, it is clear that if a totally skew-symmetric isotope $\mathfrak{A}_o$ of $\mathfrak{A}$ is given by $xoy=(x^U\cdot y^V)^W$, and if $\mathfrak{A}_o$ has linear sets $\mathfrak{X}_o$, $\mathfrak{Y}_o$ of orders x, $n-r$ respectively such that $xoy=0$ for every x of $\mathfrak{X}_o$ and y of $\mathfrak{Y}_o$, then there exist sets $\mathfrak{X}$ and $\mathfrak{Y}$ of corresponding orders with the same property for $\mathfrak{A}$, and conversely. In fact $\mathfrak{X}$ can be taken to be the set of all elements x^P with $P=U^{-1}$, x in $\mathfrak{X}_o$, and $\mathfrak{Y}$ to be the set of all elements x^Q with $Q=V^{-1}$, y in $\mathfrak{Y}_o$.

Corollary 2 may be proved by using Theorem 4D along with the well known fact that $x\cdot y=0$ for a nonzero vector x of three-dimensional space if and only if y is parallel to x. The reader should also verify that this vector algebra is a Lie algebra, or that

$$x^2=0, \qquad xy=-yx, \qquad x\cdot yz+y\cdot zx+z\cdot xy=0. \tag{4.15}$$

The Lie algebras, which we see by (4.15) to be anti-commutative, are the best known of all non-associative algebras, and the simple Lie algebras have been determined, at least for fields of characteristic zero. (For references to the literature, see [8, p. 188, §8].) We shall now consider the isotopic simplicity of certain of these algebras. Note that if $\mathfrak{L}$ is any set of n-rowed square matrices closed under the multiplication

$$AoB=AB-BA, \tag{4.16}$$

then $\mathfrak{L}$ satisfies (4.15) and hence is a Lie algebra.

THEOREM 4E. (i) *The Lie algebra $\mathfrak{S}_n$ of order $n(n-1)/2$, consisting of all skew-symmetric matrices, over any subfield $F=R$ of the field of all reals, under the multiplication* (4.16), *is isotopically simple.*

(ii) *The Lie algebra $\mathfrak{H}_n$ of order $n(n-1)$, consisting of all skew-hermitian matrices in any field $F=R(i)$ (where R is a subfield of the reals and $i^2=-1$), under the multiplication* (4.16), *is an isotopically simple algebra over R.*

Proof. By definition, A is skew-symmetric if its transpose A' is equal to $-A$, and skew-hermitian if its conjugate transpose $A^*=\overline{A}'$ is equal to $-A$. If A, B are skew-symmetric, it is readily verified that AoB is skew-symmetric, and hence that $\mathfrak{S}_n$ is a Lie algebra. Similarly $\mathfrak{H}_n$ is a Lie algebra. The basis of both $\mathfrak{S}_n$ and $\mathfrak{H}_n$ may be taken to be the set of matrices f_{ij} with $i<j$, where $f_{ij}=e_{ij}-e_{ji}$ and the e_{ij} are the usual canonical basis of $\mathfrak{M}_n$. Both algebras, moreover, are totally skew-symmetric relative to this basis, and hence the criterion of Theorem 4D may be employed in our proof.

If $\mathfrak{S}$ is any set of n-rowed skew-symmetric matrices over R, containing exactly s linearly independent matrices, and if $\mathfrak{T}$ is the set of order t, consisting of all skew-symmetric matrices over R which commute with every matrix of $\mathfrak{S}$, we wish to show that $s+t$ is less than $n(n-1)/2$. But if we consider $\mathfrak{S}$ over the field K of all complex numbers, the linear order of $\mathfrak{S}$ relative to K

will still be s, the matrices of $\mathfrak{S}$ will be skew-hermitian (since they are real and skew-symmetric) and the set $\mathfrak{T}_1$ consisting of all skew-hermitian matrices commutative with $\mathfrak{S}$ will contain $\mathfrak{T}$ and hence have order $t_1 \geqq t$. Hence it will be sufficient to show $s+t_1<n(n-1)/2$. Since a similar remark may be made in connection with skew-hermitian matrices over a field $R(i)$, we shall henceforth consider only skew-hermitian matrices over K.

If $\mathfrak{S}_1$ is any set of skew-hermitian matrices over K, let $\mathfrak{B}$ be the commutator algebra of $\mathfrak{S}_1$, and $\mathfrak{A}$ the commutator algebra of $\mathfrak{B}$. The set $\mathfrak{S}$, consisting of all skew-hermitian matrices in $\mathfrak{A}$, contains $\mathfrak{S}_1$ and is moreover a Lie algebra under the multiplication (4.16). Similarly the set $\mathfrak{T}$ of all skew-hermitian matrices in B is a Lie algebra under (4.16). Moreover $\mathfrak{T}$ consists of all skew-hermitian matrices commutative with $\mathfrak{S}_1$, and $\mathfrak{S}$ of all skew-hermitian matrices commutative with $\mathfrak{T}$. We shall use without proof the following well known result [9].

LEMMA 4B. *A set $\mathfrak{S}_1$ of skew-hermitian matrices over the complex field is completely reducible. In fact there exists a unitary matrix U ($U^* = U^{-1}$) such that $U\mathfrak{S}_1 U^*$ is in completely reduced form.*

Since $U\mathfrak{S}_1U^*$ consists of skew-hermitian matrices we shall assume that $\mathfrak{S}_1$ itself is in completely reduced form:

$$\mathfrak{S}_1 = \begin{pmatrix} I_{r_1} \times \mathfrak{P}_1 & & \\ & \ddots & \\ & & I_{r_p} \times \mathfrak{P}_p \end{pmatrix},$$

where I_r is the r-rowed unit matrix and $\mathfrak{P}_i$ is an irreducible set of s_i-rowed skew-hermitian matrices, with $\mathfrak{P}_i$ not equivalent to $\mathfrak{P}_j$ for $i \neq j$. Since the complex field K is algebraically closed the only s_i-rowed matrices commutative with $\mathfrak{P}_i$ are the scalar multiples of the unit matrix I_{s_i}. Hence the algebras $\mathfrak{B}$ and $\mathfrak{A}$ described above are given by

$$(4.17)\quad \mathfrak{A} = \begin{pmatrix} I_{r_1} \times \mathfrak{M}_{s_1} & & \\ & \ddots & \\ & & I_{r_p} \times \mathfrak{M}_{s_p} \end{pmatrix}, \quad \mathfrak{B} = \begin{pmatrix} \mathfrak{M}_{r_1} \times I_{s_1} & & \\ & \ddots & \\ & & \mathfrak{M}_{r_p} \times I_{s_p} \end{pmatrix}.$$

Thus if $\mathfrak{H}_r$ is the irreducible set consisting of all skew-hermitian matrices of r rows and columns, the sets $\mathfrak{S}$ and $\mathfrak{T}$ corresponding to $\mathfrak{A}$ and $\mathfrak{B}$ are

$$(4.18)\quad \mathfrak{S} = \begin{pmatrix} I_{r_1} \times \mathfrak{H}_{s_1} & & \\ & \ddots & \\ & & I_{r_p} \times \mathfrak{H}_{s_p} \end{pmatrix}, \quad \mathfrak{T} = \begin{pmatrix} \mathfrak{H}_{r_1} \times I_{s_1} & & \\ & \ddots & \\ & & \mathfrak{H}_{r_p} \times I_{s_p} \end{pmatrix}.$$

Our proof will be complete if we show $s+t<n(n-1)/2$, where s, t are the respective linear orders of $\mathfrak{S}$ and $\mathfrak{T}$. But

$$\begin{aligned} 2s &= s_1(s_1-1)+\cdots+s_p(s_p-1),\\ 2t &= r_1(r_1-1)+\cdots+r_p(r_p-1), \qquad (4.19)\\ n &= r_1s_1+\cdots+r_ps_p. \end{aligned}$$

We assume of course that each integer r_i, s_i is greater than zero. Now, for any two positive integers f, g,

$$(4.20)\qquad fg(fg-1)-f(f-1)-g(g-1)=(f-1)(g-1)(fg+f+g);$$

and hence if $p=1$, $s_1=f$, $r_1=g$, $n=fg$ we have $n(n-1)>s_1(s_1-1)+r_1(r_1-1)$ except when one of f, g has the value 1. But this case occurs only when one of $\mathfrak{S}$, $\mathfrak{T}$ consists solely of the zero matrix, a situation of no interest in connection with the criterion of Theorem 4D. Aside from this trivial case, therefore, we have $s+t<n(n-1)/2$ when $p=1$. In case p is greater than one, we use the fact that $a>0$, $b>0$ implies

$$(4.21)\qquad (a+b)(a+b-1)>a(a-1)+b(b-1).$$

(Indeed the left side of (4.21) exceeds the right side by $2ab$.) Since each product r_is_i is positive we may employ an extension of (4.21), along with (4.20), to obtain from (4.19) the following:

$$\begin{aligned} n(n-1)-2(s+t) &> \sum\left[r_is_i(r_is_i-1)-r_i(r_i-1)-s_i(s_i-1)\right]\\ &= \sum (r_i-1)(s_i-1)(r_is_i+r_i+s_i)\\ &\geqq 0. \end{aligned}$$

Thus we derive $s+t<n(n-1)/2$, with which Theorem 4E is proved.

5. **Isotopically indecomposable algebras.** If every element x of an algebra $\mathfrak{A}$ is uniquely expressible in the form $x=x_1+x_2$ where x_1, x_2 belong respectively to the invariant subalgebras (or ideals) $\mathfrak{A}_1$, $\mathfrak{A}_2$ of $\mathfrak{A}$ we say that $\mathfrak{A}$ is *decomposable* into $\mathfrak{A}_1$ and $\mathfrak{A}_2$ and that $\mathfrak{A}$ is a *direct sum* of $\mathfrak{A}_1$ and $\mathfrak{A}_2$, $\mathfrak{A}=\mathfrak{A}_1\oplus\mathfrak{A}_2$. If $\mathfrak{A}$ is not decomposable then $\mathfrak{A}$ is *indecomposable.* We may state without proof the following theorem, since the proof is not essentially different from that of Theorem 2A.

THEOREM 5A. *A necessary and sufficient condition that a non-associative algebra $\mathfrak{A}$ be indecomposable is that the corresponding associative algebra of transformations $E(\mathfrak{R}, \mathfrak{L})$ be indecomposable.*

An algebra $\mathfrak{A}$ is *isotopically indecomposable* if and only if it possesses no isotope which is decomposable. In particular, isotopically simple algebras are isotopically indecomposable.

THEOREM 5B. *If an indecomposable algebra $\mathfrak{A}$ has a unit element, then $\mathfrak{A}$ is isotopically indecomposable.*

Proof. Let $\mathfrak{A}_o$ be a principal isotope of $\mathfrak{A}$, $xoy=x^U\cdot y^V$. Then $\mathfrak{R}_o=U\mathfrak{R}$,

$\mathfrak{L}_o = V\mathfrak{L}$. Since $\mathfrak{R} \supset I$, $\mathfrak{R}_o \supset U$, and hence $E(\mathfrak{R}_o) \supset U$, U^{-1}, $E(\mathfrak{R})$. Thus $E(\mathfrak{R}_o) = E(U, \mathfrak{R})$. Similarly $E(\mathfrak{L}_o) = E(V, \mathfrak{L})$ and $E(\mathfrak{R}_o, \mathfrak{L}_o) = E(U, V, \mathfrak{R}, \mathfrak{L})$. It follows that if $\mathfrak{A}_o$ is decomposable the same must be true of $\mathfrak{A}$, contrary to hypothesis.

THEOREM 5C. *Every algebra $\mathfrak{A}$ possesses an isotope $\mathfrak{B}$ which is decomposable into a direct sum of a finite number of isotopically indecomposable algebras.*

Proof. If $\mathfrak{A}$ is isotopically indecomposable the theorem is proved. Otherwise $\mathfrak{A}$ has an isotope, let us say $\mathfrak{A}$ itself, which is decomposable, $\mathfrak{A} = \mathfrak{A}_1 \oplus \mathfrak{A}_2$. Since we may now apply isotopic transformations separately to $\mathfrak{A}_1$ and $\mathfrak{A}_2$ the proof may be completed by induction upon the (finite) order of $\mathfrak{A}$.

Theorem 4B, part (iii), may be modified in an obvious manner so as to give necessary and sufficient conditions on the trilinear form $F(x, y, z)$ that $\mathfrak{A}$ should have a decomposable isotope. However nothing seems to be gained in simplicity over the matrix form of the same thing.

6. **Quasigroup algebras.** In the early papers on linear algebras (those for example of Hamilton, Cayley, Graves, Gibbs, Clifford, and Shaw; we shall not give references) one frequently encounters the notion of *units*. By a set of units is generally meant a basis $e_1, e_2, \cdots, e_n$ of the algebra such that each product e_ie_j is of the form $\alpha \cdot e_k$ where α is a rational number, usually 0 or ± 1. We shall single out some famous examples.

(a) Three algebras $(1, i)$ with unit element 1: the complex numbers $(i^2 = -1)$, the dual numbers $(i^2 = 0)$, and the Clifford numbers $(i^2 = +1)$.

(b) Gibb's algebra (i, j, k) of three-dimensional vectors $(i^2 = j^2 = k^2 = 0$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j)$.

(c) Hamilton's quaternions $(1, i, j, k)$ with unit element 1 $(i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j)$.

(d) The Cayley-Graves-Dickson division algebra of order 8. (The multiplication table of this algebra is too complicated to give here; see [10, p. 14].)

In connection with some researches into division algebras, the author was led to define *quasigroup algebras*, as follows. Let Q be a group or quasigroup, usually of finite order. To every element p of Q let there correspond an element u_p of an algebra $\mathfrak{A}$ such that the u_p form (in the usual sense) a linearly independent basis of $\mathfrak{A}$ over a field F. Finally define multiplication in $\mathfrak{A}$ by

$$u_p \cdot u_q = h_{p,q} \cdot u_{pq}, \tag{6.1}$$

where the $h_{p,q}$ are nonzero elements of F and pq designates multiplication in Q The resultant algebra we call a quasigroup algebra, or, in case Q is a group, a group algebra.

It is to be emphasized that a quasigroup algebra is quite distinct from a crossed product; in fact the elements of F are both associative and commutative with the basis elements u_p. However if a group G has a normal subgroup H, the group algebra associated with G can be regarded in a certain sense as a crossed extension of the algebra associated with H. For example, the complex numbers $\mathfrak{K}$ are associated with the two-group G_2, the quaternions $\mathfrak{Q}$ with $G_4=G_2\times G_2$, and the Cayley-Dickson numbers $\mathfrak{C}$ with $G_8=G_2\times G_4$; moreover $\mathfrak{Q}$ is a crossed extension of $\mathfrak{K}$, and $\mathfrak{C}$ is a crossed extension of either $\mathfrak{K}$ or $\mathfrak{Q}$. In view of Heinz Hopf's theorem [11, p. 225, Satz 1E] that every division algebra over the field of all real numbers has order 2^p for some p, the author has taken a special interest in the group algebras associated with the pth power $G_2{}^p$ of G_2.

7. **Quasigroup rings.** A quasigroup algebra in which the $h_{p,q}$ of equation (6.1) are all equal to the identity of the underlying field F is called a *quasigroup ring*. The proof of the first statement of the following theorem was suggested to the author by D. C. Murdoch.

THEOREM 7A. *Every quasigroup ring $\mathfrak{Q}$ defined over a non-modular field F by a finite quasigroup Q is a direct sum of simple algebras. Each such simple component of $\mathfrak{Q}$ is either isotopically simple or isotopic to a determinate number of isotopically simple algebras, each with a unit element.*

As we shall see in the proof, the theorem is also true for certain modular fields, depending on Q. The equations

$$pq = p^{R_q} = q^{L_p} \tag{7.1}$$

associate with each element p of Q a right-permutation R_p and a left-permutation L_p (compare [3] and [4]). The permutation group generated by all the R_p and L_p we denote by G. If Q has order n and G order m, then we have $n\leqq m\leqq n!$. Moreover m is a divisor of $n!$. A. Suschkewitsch [12] has essentially shown, in somewhat disguised form, that the equality $m=n$ can hold if and only if Q is a group isomorphic to G (see also [3]). We shall therefore leave aside this case and assume $m>n$, since the situation for groups is well known.

The quasigroup ring $\mathfrak{Q}$ is isomorphic to the linear closure of Q, and-we might as well let the elements p, q of Q form a basis of $\mathfrak{Q}$. If G be regarded as an abstract group, then the group ring of G is represented by an algebra $E(G)\equiv E(\mathfrak{R}, \mathfrak{L})$ of n-rowed square matrices, where $\mathfrak{R}$ for example is the linear set consisting of all linear combinations of the R_p, regarded as linear transformations. Moreover $E(G)$ is the usual polynomial algebra associated with the algebra $\mathfrak{A}=\mathfrak{Q}$. The fact that m is greater than n shows that $E(G)$, of order n, is not the regular representation of the group ring of G. We are interested in the case that $E(G)$ is completely reducible, a sufficient condition for which is that the characteristic of F be prime to m; certainly then we are safe if F has characteristic zero, or prime characteristic greater than n.

But if $E(G)$ is completely reducible, then $\mathfrak{Q}$ is a direct sum of simple algebras, equal in number to the number of irreducible constituents of $E(G)$. This proves the first statement of the theorem.

If a, b are fixed elements of Q, we may define a quasigroup Q_o, a principal isotope of Q with a unique unit element ab, by

$$poq = p^{R_b^{-1}} \cdot q^{L_a^{-1}}; \tag{7.2}$$

moreover, every isotope with a unit element of Q is isomorphic to some such Q_o [3, 4]. At the same time (7.2) may be used to define a quasigroup ring $\mathfrak{Q}_o$ isotopic to $\mathfrak{Q}$, namely the ring defined by Q_o. Since R_b^{-1} and L_a^{-1} are in $E(G)$, $E(G_o)$ will have constituent corresponding to the constituent of $E(G)$, but not necessarily irreducible. But it follows readily that, since $E(G_o)$ is completely reducible, each such reducible constituent of $E(G_o)$ will itself be completely reducible. In view of the fact that Q_o has a unit element, we have now essentially proved the second statement of Theorem 7A. However we might refer the reader to a theorem of Albert [2, Theorem 10, p. 699] in order to be able to round out the proof with the remark that *if two semi-simple quasigroup rings, each with a unit element, are isotopic, then their simple parts are isotopic in pairs.* (Following Albert, we say an algebra is semi-simple if it is a direct sum of simple algebras.)

It might be of interest to note that the group G_o associated with Q_o is a subgroup of G. This follows since G_o is generated by the permutations

$$\overset{o}{R_q} = \overset{-1}{R_b} R_t, \qquad \overset{o}{L_p} = \overset{-1}{L_a} L_s$$

where

$$t = q^{L_a^{-1}}, \qquad s = p^{R_b^{-}}.$$

As a simple illustration of the above theory, consider the following quasigroup Q of order 3:

(7.3)

	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

Here $R_1 = L_1 = (23)$, $R_2 = L_2 = (13)$, $R_3 = L_3 = (12)$, and G is the symmetric group of order 6. The ring $E(G)$, of order 3, contains just two irreducible representations of G, each once. Indeed the alternating representation, with its generating idempotent

$$(1/6)[1 - (12) - (13) - (23) + (123) + (132)],$$

is mapped upon zero. It may easily be shown that if the underlying field has characteristic different from 3, then $\mathfrak{Q}$ is a direct sum of the field F and a commutative algebra $\mathfrak{A} = (e, f)$ with multiplication table

$$e^2 = e, \qquad f^2 = f, \qquad ef = fe = -e - f. \tag{7.4}$$

If, in addition, -3 is a non-square in F, $\mathfrak{A}$ is a division algebra, and hence isotopically simple, but otherwise $\mathfrak{A}$ has an isotope which is a direct sum of two algebras isomorphic to F. It was this example, encountered in quite another connection, which suggested the notion of quasigroup algebras.

8. **Simple quasigroup algebras.** In this section we restrict attention to quasigroups Q which have a unit element 1 and moreover possess the *inverse property*. Such a quasigroup Q [4, §3] possesses a one-to-one reversible mapping $p \to p^J = p^{-1}$ such that

$$(8.1) \qquad p \cdot p^{-1} = p^{-1} \cdot p = 1, \qquad pq \cdot q^{-1} = q^{-1} \cdot qp = p$$

for all p, q of Q. Since Q has a unit element, we shall use Albert's term *loop* [3] and refer to it as a *loop with the inverse property*. In particular, Q may be a group.

Theorem 8A. *Let Q be a finite loop with the inverse property, let F be a field, and let $\mathfrak{A}$ be a loop algebra, corresponding to Q and F, with unit element u_1 and multiplication defined by* (6.1). (i) *If F has only two elements, $\mathfrak{A}$ may not be semi-simple.* (ii) *If Q has order two, $\mathfrak{A}$ is simple if and only if it is a field.* (iii) *If both F and Q have at least three elements, the $h_{p,q}$ can always be chosen so that $\mathfrak{A}$ is right-simple or left-simple or both; for suitable choices see below.*

Proof. (i) In this case any quasigroup algebra is a quasigroup ring, and will be semi-simple if and only if the order of the group associated with Q is prime to 2, that is, odd.

(ii) See the first part of the proof of Theorem 3E.

(iii) We shall show that the following conditions are sufficient for left-simplicity and right-simplicity respectively. Note that $h_{p,1} = h_{1,p} = 1$, since u_1 is the unit element of $\mathfrak{A}$.

For left-simplicity. Assume that for every $p \neq 1$ of Q there is at least one $q \neq 1$ such that $u_q(u_{q^{-1}}u_p)$ is not equal to $(u_q u_{q^{-1}}) \cdot u_p$. This means

$$(8.2) \qquad h_{q,q^{-1}p} \cdot h_{q^{-1},p} \neq h_{q,q^{-1}}.$$

Let

$$(8.3) \qquad x = \alpha_1 u_1 + \cdots + \alpha_p u_p + \cdots,$$

where the α_p are elements of F, be an arbitrary nonzero element of $\mathfrak{A}$, and designate by Λ_x the left-ideal generated by x. As a temporary convenience let us call an element x *prepared* if α_1 is not equal to 0, and let us define the *length* of x to be the number of nonzero coefficients $\alpha_1, \cdots, \alpha_p, \cdots$. Now Λ_x contains a prepared element, which we may as well assume to be x, for if α_p is not equal to 0 then $y = u_{p^{-1}} \cdot x$ is prepared. (Moreover y and x have the same length, and also $\Lambda_x = \Lambda_y$.) If then x is prepared, either x has length one or $\alpha_p \neq 0$ for some $p \neq 1$. Consider the second case. By hypothesis there exists a $q \neq 1$ such that $u_q(u_{q^{-1}}u_p)$ is not equal to $(u_q u_{q^{-1}})u_p$. Consider the element

$$z = (u_q u_{q^{-1}})x - u_q(u_{q^{-1}}x).$$

Then z is not equal to 0, since the coefficient of u_p is not equal to 0. Moreover z has length less than the length of x, since no new nonzero coefficients are added, and indeed

$$\begin{aligned}(u_qu_{q^{-1}})\cdot\alpha_1u_1 - u_q(u_{q^{-1}}\cdot\alpha_1u_1) &= \alpha_1u_1[h_{q,q^{-1}}h_{1,1} - h_{q,q^{-1}}h_{q^{-1},1}]\\ &= \alpha_1u_1(h_{q,q^{-1}} - h_{q,q^{-1}})\\ &= 0.\end{aligned}$$

Then $\Lambda_x \supset \Lambda_z$, where z has shorter length than x. By induction we may show that Λ_x contains u_1 and hence $\mathfrak{A}$. Thus $\mathfrak{A}$ is left-simple.

For right-simplicity. Assume that for every $p\neq 1$ *of* Q *there exists at least one* $q\neq 1$ *such that* $(u_pu_{q^{-1}})u_q$ *is different from* $u_p(u_{q^{-1}}u_q)$. This means

$$h_{p,q^{-1}}\cdot h_{pq^{-1},q} \neq h_{q^{-1},q}. \tag{8.4}$$

The proof in this case follows the same lines as before. Under the hypothesis of the theorem we may satisfy both conditions simultaneously by setting

$$u_1\cdot u_1 = u_1, \qquad u_1\cdot u_p = u_p\cdot u_1 = u_p, \qquad u_pu_q = h\cdot u_{pq}, \tag{8.5}$$

where p, q are not equal to 1 and h is not equal to 0, 1. As a check note that

$$(u_pu_{q^{-1}})\cdot u_q = h^2\cdot u_p, \qquad u_p\cdot(u_{q^{-1}}u_q) = h\cdot u_p$$

and hence these are distinct if $h^2\neq h$ or $h\neq 0$, 1.

9. **Truncated loop algebras.** In the study of linear algebras the notion of constructing a difference algebra $\mathfrak{A}-\mathfrak{B}$ is familiar enough in the case that $\mathfrak{B}$ is an ideal of $\mathfrak{A}$. However such an algebra may still be constructed when $\mathfrak{B}$ is any subset of $\mathfrak{A}$ (see for example [13, p. 37]), provided we are willing to relinquish the property that $\mathfrak{A}-\mathfrak{B}$ should be a homomorph of $\mathfrak{A}$. We here define a *truncated loop algebra* to be a loop algebra taken modulo its unit element (in a sense to be made more precise in a moment) and derive a theorem which yields in particular the following somewhat bizarre result: *The group ring of any finite group, when taken modulo its unit element, is both right simple and left simple.*

If Q is any loop with unit element 1, designate by Q' the set consisting of all elements of Q except 1. Consider the algebra $\mathfrak{A}$ with linearly independent basis $(u_p, p\subset Q')$ over a field F, where

$$u_pu_q = \begin{cases} h_{p,q}u_{pq} & \text{if } pq \subset Q',\\ 0 & \text{if } pq = 1,\end{cases} \tag{9.1}$$

and where $h_{p,q}$, for $pq\subset Q'$, is a nonzero element of F. Such an algebra $\mathfrak{A}$ we call a *truncated loop algebra*, or, in case all the $h_{p,q}$ have the value $+1$, a *truncated loop ring.*

THEOREM 9A. *Let* Q *be a finite loop with the inverse property, of order* $n\geqq 2$.

Then there exists a truncated loop algebra $\mathfrak{A}$ corresponding to Q, over an arbitrary field, which is both right simple and left simple. In particular a truncated loop ring, corresponding to any finite loop with the inverse property, is both right simple and left simple.

Proof. It is readily seen that the right or left ideal generated by a basis element u_p of $\mathfrak{A}$ coincides with $\mathfrak{A}$. We shall determine the $h_{p,q}$ so that the right or left ideal generated by any nonzero element

$$x = \sum \alpha_p u_p, \qquad p \subset Q', \tag{9.2}$$

contains a basis element and hence $\mathfrak{A}$. Since x is not equal to 0, we have $\alpha_q \neq 0$ for some q. Thus

$$x u_{q^{-1}} = \sum_p \alpha_p h_{p,q^{-1}} u_{pq}, \qquad p \neq q,$$

and

$$(x u_{q^{-1}}) u_q = \sum_p \alpha_p h_{p,q^{-1}} h_{pq^{-1},q} u_p, \qquad p \neq q. \tag{9.3}$$

We make the assumption that

$$h_{p,q^{-1}} \cdot h_{pq^{-1},q} = b_{q^{-1}}$$

or that

$$h_{p,q} \cdot h_{pq,q^{-1}} = b_q, \tag{9.4}$$

for all distinct pairs p^{-1}, q of Q', where $b_q \neq 0$ is independent of p. Then from (9.2), (9.3), and (9.4) we derive

$$b_{q^{-1}} \cdot x - (x u_{q^{-1}}) u_q = b_{q^{-1}} \cdot \alpha_q u_q.$$

It follows that the right ideal generated by x contains u_q and hence coincides with $\mathfrak{A}$. Thus $\mathfrak{A}$ is right simple if (9.4) is satisfied. Similarly the equation

$$h_{p,q} h_{p^{-1},pq} = a_p, \tag{9.5}$$

which is to hold for all distinct pairs p^{-1}, q of Q', where $a_p \neq 0$ is independent of q, is a sufficient condition that $\mathfrak{A}$ be left simple. If Q has order two, conditions (9.4), (9.5) are impossible, but nevertheless $\mathfrak{A}$ is simple, since it is the zero algebra of order one. If we set $a_p = b_p = h_{p,q} = 1$ for $pq \neq 1$, the conditions (9.4) and (9.5) are clearly satisfied, and hence *a truncated loop ring, defined by a finite loop with the inverse property, is right and left simple.* This completes the proof of Theorem 9A.

Let Q be a unipotent loop with the inverse property; that is, a loop with the inverse property in which $p^2 = 1$ or $p^{-1} = p$ for every p of Q [4, §7]. It is shown in [4] that Q must be commutative; in fact Q is a so-called *unipotent totally symmetric quasigroup.* If we assume

$$h_{p,q} = - h_{q,p} \neq 0, \qquad p \neq q, \tag{9.6}$$

for p, q in Q', then (9.4) and (9.5) reduce to

$$h_{p,q}h_{p,pq} = a_p = b_p \neq 0, \qquad p \neq q. \tag{9.7}$$

If (9.6) and (9.7) are simultaneously satisfied, not only will $\mathfrak{A}$ be right and left simple but it will be of class (IV), since we will have $x^2=y^2=xy+yx=0$ for every x, y of $\mathfrak{A}$. (It should be noted that (9.6) is impossible unless Q is unipotent.) Moreover, $\mathfrak{A}$ will be anti-commutative. It is easily seen that the further condition that $\mathfrak{A}$ should be totally skew-symmetric is

$$h_{p,pq} = -h_{p,q}; \tag{9.8}$$

in fact this implies that if $u_pu_q=-u_qu_p=c\cdot u_r$ then $u_qu_r=-u_ru_q=cu_p$ and $u_ru_p=-u_pu_r=cu_q$. But (9.8) coupled with (9.7) gives

$$a_p = -h_{p,q}^2 = -h_{q,p}^2 = a_q, \qquad p \neq q,$$

whence

$$a_p = -a^2 \neq 0, \tag{9.9}$$

where the constant a is independent of p. In this case we may define a new basis (v_p) by $av_p=u_p$ and get

$$v_pv_q = k_{p,q}v_q \qquad (p \neq q)$$

where the $h_{p,q}$ may be replaced by the $k_{p,q}$ in (9.6), (9.7), (9.8) provided a_p is replaced by -1. Thus we see that without loss of generality these equations may be replaced by

$$h_{p,q} = -h_{p,pq} = -h_{q,p}, \qquad h_{p,q}^2 = 1 \qquad (p \neq q) \tag{9.10}$$

which implies

$$h_{p,q} = h_{q,pq} = h_{pq,p} = -h_{q,p} = -h_{p,pq} = -h_{pq,q} = \pm 1, \tag{9.11}$$

for $p \neq q$. Now in a unipotent totally symmetric loop of (even) order n, any two distinct elements p, q, neither of which is the identity, generate a subloop of order 4, namely the four-group $(1, p, q, pq)$, which would also be generated by any two of the three elements p, q, pq. It follows that there exist exactly $(n-1)(n-2)/6$ such subloops. Every four-group $(1, p, q, pq)$ defines six constants h, as indicated by (9.11); moreover, if any one of the six be given one of the values ± 1, the others are uniquely determined. Thus we have the following.

THEOREM 9B. *Let Q be a unipotent loop with the inverse property, of finite order $n \geqq 4$. Then there exists a simple truncated loop algebra $\mathfrak{A}$, associated with Q, which is a totally skew-symmetric algebra of order $n-1$ and class* (IV). *In fact the constants $h_{p,q}$, $(n-1)(n-2)$ in number, may be divided into sets of six, as indicated by* (9.11), *where the $+1$ or -1 in that formula may be chosen at will for each set. For each choice the corresponding algebra is simple.*

When $n=4$, the $\mathfrak{A}$ of Theorem 9B is the algebra of three-dimensional vectors, which we have shown (Theorem 4D, Corollary 2) to be *isotopically* simple. It would seem to be highly desirable to settle the question of isotopic simplicity for the general case of Theorem 9B, but this, up to the time of writing, we have been unable to do.

10. Quasigroup extensions. It would appear that G. N. Garrison [14, §4, pp. 480–487] was the first to give a wholly satisfactory theory of homomorphisms and coset expansions of a finite quasigroup. This he developed in terms of his *invariant complexes*. More recently, A. A. Albert has given a corresponding theory for loops of finite or infinite order, and, in a second paper, has solved the general extension problem for loops [3, I, II]. We here give our own solution of the general extension problem for arbitrary quasigroups. This was obtained in August 1942, at the suggestion and with the help of D. C. Murdoch, and was applied to the construction of division algebras, as we shall show in later sections. The account which we now present differs in many details from that of Albert, which we have seen in manuscript; indeed it might rather be regarded as a natural modification and development of the ideas of Garrison.

Let H be any set of elements $a, b, c, \cdots$. We shall define the *order* m of H to be its cardinal number, finite or transfinite. Let Q be set of order n, with elements $p, q, \cdots$, which forms a quasigroup under the multiplication pq. Suppose that, corresponding to every ordered pair p, q of elements of Q, there has been defined in any manner a quasigroup $H_{p,q}$, consisting of the elements of H under the multiplication $(a\cdot b)_{p,q}$. (The subscripts p, q serve to point out that the ordered product of a and b in $H_{p,q}$ depends in general upon p and q.) Consider the set R of all element pairs (a, p) with a in H, p in Q. Then R has order mn. If multiplication in R be defined by

$$(10.1) \qquad (a, p)(b, q) = ((ab)_{p,q}, pq),$$

then R is a quasigroup, which we shall call an *extension of H by Q*. In fact, the equation

$$(10.2) \qquad (a, p)(b, q) = (c, r)$$

is equivalent to the two equations

$$(10.3) \qquad (a\cdot b)_{p,q} = c, \qquad pq = r.$$

But, since Q is a quasigroup, if any two of p, q, r be given as elements of Q, the third is uniquely determined from (10.3) as an element of Q. Moreover, if p, q are known elements of Q, and if any two of a, b, c be given as elements of $H_{p,q}$ (that is, H), the third is uniquely determined from (10.3) as an element of $H_{p,q}$. It follows that if any two of the three element pairs appearing in (10.2) be given as elements of R the third is uniquely determined as an element of R. Thus R is a quasigroup under (10.1). We have thus proved the first statement of the following theorem.

THEOREM 10A. *The quasigroup extension $R=(H, Q)$, defined above, of a set H of order m by a quasigroup Q of order n (these orders being finite or transfinite) is a quasigroup of order mn. Moreover R is homomorphic to Q. Conversely, if a quasigroup R is homomorphic to a quasigroup R', then R may be exhibited as an extension (H, Q) where Q is isomorphic to R'.*

Proof. The first statement of the Theorem 10A has been dealt with above. Next we note that if H_p denotes the set of all elements (a, p) with a in H, we have from (10.1) and the fact that $H_{p,q}$ is a quasigroup the following result:

$$H_p \cdot H_q = H_{pq}. \tag{10.4}$$

Thus the mapping $(a, p) \rightarrow H_p$ is a homomorphism of $R=(H, Q)$ upon a quasigroup isomorphic to Q.

Assume conversely that R is an arbitrary quasigroup homomorphic to a quasigroup R' under the mapping

$$p \rightarrow p', \qquad q \rightarrow q', \qquad pq \rightarrow (pq)' = p'q', \tag{10.5}$$

it being understood that to every element r' of R' there corresponds at least one r of R such that $r \rightarrow r'$ under (10.5). Designate by $H_{r'}$ the set of all elements r in R which map into r'. Then, as we shall show, if $H_{p'} \cdot H_{q'}$ denotes the usual set product in R, we have

$$H_{p'} \cdot H_{q'} = H_{p'q'}, \tag{10.6}$$

so that the sets $H_{p'}$, under set multiplication, form a quasigroup isomorphic to R. On the one hand we see from (10.5) that $p \subset H_{p'}$, $q \subset H_{q'}$ implies $pq \subset H_{p'q'}$; hence $H_{p'} \cdot H_{q'} \subset H_{p'q'}$. On the other hand, if $r \subset H_{p'q'}$ and $p \subset H_{p'}$, we may determine a unique element u of R so that $pu=r$. Thus by (10.5), $p'u'=r'=p'q'$, whence $u'=q'$, $u \subset H_{q'}$. (Similarly, to every q of $H_{q'}$ and r of $H_{p'q'}$ there corresponds a unique p of $H_{p'}$ such that $pq=r$.) In particular we have $H_{p'q'} \subset H_{p'} H_{q'}$; and (10.6) is proved.

In connection with the proof of (10.6) we have actually proved more, namely that *each set $H_{p'}$ has the same order m, finite or transfinite.* For if $H_{p'}$, $H_{q'}$ are any two such sets, we may use any fixed element r of $H_{p'q'}$ to set up a one-to-one correspondence $p \rightleftarrows q$ between the full sets $H_{p'}$, $H_{q'}$ by stating that p of $H_{p'}$ shall correspond to q of $H_{q'}$ if and only if $pq=r$. Thus $H_{p'}$ and $H_{q'}$ have the same cardinal number. Note also that, by their very definition, $H_{p'}$ and $H_{q'}$ can only have common elements when $p'=q'$.

If f is any fixed element of R, let us write $H=H_{f'}$. If p' is any element of R' there exists a unique element s' of R' such that $f's'=p'$ and hence $H \cdot H_{s'}=H_{p'}$. Suppose that, by appeal if necessary to the axiom of choice, we have selected for each p' an element P in the corresponding $H_{s'}$. Then we have

$$H \cdot P = H_{p'}. \tag{10.7}$$

The correspondence $P \rightleftarrows p'$ will be an isomorphism of a quasigroup Q upon R', provided we define a new product by which $P \cdot Q = R$ if $P \rightleftarrows p'$, $Q \rightleftarrows q'$, and $R \rightleftarrows p'q'$. Finally, if a, b, c designate elements of H, the equation

$$aP \cdot bQ = c \cdot PQ, \tag{10.8}$$

which is simply another form of (10.6), is such that any two of a, b, c uniquely determine the third. Thus if we write

$$c = (ab)_{P,Q}, \tag{10.9}$$

(10.8) corresponds exactly to (10.1), except that couples (a, p) have been replaced by products aP. This completes the proof of Theorem 10A.

In order to bring the present theory in closer accord with Albert's work, we now consider the case of loops.

THEOREM 10B. *In the notation of this section, the following conditions are necessary and sufficient in order that an extension $R = (H, Q)$ of a set H by a quasigroup Q should be a loop:*

(i) *Q must be a loop with unit element* 1.

(ii) *$H_{1,1}$ must be a loop with a unit element e which is a left unit for every $H_{1,q}$ and a right unit for every $H_{p,1}$.*

If these conditions are satisfied the element $(e, 1)$ is the unit element of the loop R. Moreover we may identify H with the subloop $H_{1,1}$ of R, and speak of (H, Q) as a loop extension of a loop H by a loop Q.

Proof. We leave it to the reader to show that the conditions are sufficient. As to their necessity, let $(e, 1)$ be the unit element of a loop $R = (H, Q)$. Then from (10.1) and (10.3), if $(e, 1) \cdot (b, q) = (b, q)$ we have

$$(eb)_{1,q} = b, \qquad 1q = q. \tag{10.10}$$

From (10.10) we see that e must be a left unit of every $H_{1,q}$, and that 1 must be a left unit of Q. Similarly, from the equation $(a, p) \cdot (e, 1) = (a, p)$ we derive that e must be a right unit of every $H_{p,1}$, and 1 a right unit of Q. It follows in particular that $H_{1,1}$ and Q are loops with units e and 1 respectively.

For the sake of completeness we shall state two theorems whose proofs we leave for a later paper. The former was obtained in order to verify a conjecture of Albert [3, II], and the latter for the purpose of relating the extension theory for general quasigroups to Albert's theory for loops.

THEOREM 10C. *Let F be an arbitrary finite loop of order $f \geqq 2$. Let G be a commutative loop of order $g \geqq 3$. Then there exists a simple loop $H = F_G$ of order $h = fg$ with the property that every proper subloop of H is a subloop of F. If $g = 2$, a loop H can be constructed whose proper subloops are subloops of F, but H is not simple.*

We remark that a quasigroup is *simple* if it cannot be exhibited as an extension (H, Q) where both H and Q have order greater than one. Since the groups of prime order are simple, and since the only loops of order four are the cyclic group and the four-group, both of which are non-simple, we now state Albert's conjecture as follows:

Corollary to Theorem 10C. *There exist simple loops of every finite order except order four.*

Theorem 10D. *Let $R=(H, Q)$ be an extension of a set H by a quasigroup Q. Then if R_o is any loop isotopic to R we have $R_o=(H_o, Q_o)$ where Q_o is a loop isotopic to Q and H_o is a set (which may be taken to be a loop) of the same order as H.*

Corollary 1. *Every isotope of a simple loop is simple.*

Corollary 2. *There exist simple quasigroups of every finite order, including order four.*

Assuming Theorem 10D and the Corollary to Theorem 10C, we establish Corollary 2 by exhibiting the following simple quasigroup of order four. If this quasigroup were non-simple, it would be homomorphic to the two-group; we leave it to the reader to verify that the contrary situation prevails.

	1	2	3	4
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

Before turning to other matters, we might note that our construction of the extension (H, Q) seems to imply a restriction on the nature of the set H, inasmuch as we have assumed the possibility of defining quasigroups on the elements of H. The restriction is only apparent. This fact may be seen from the following example for which we are indebted to S. Ulam. Let H be a set with "non-countable" cardinal number m. If U, V are any two subsets of H we may define their product $U o V$ to be the symmetric difference $U\cap V-U\cup V$, namely the set of elements in one or the other of U and V, but not in both. Under this multiplication the set $\mathfrak{A}$ of all subsets of H (including the null set) is a group. Now the number of finite subsets of H with at most f elements is $m^f=m$ for every (finite) integer f. Thus the subgroup $\mathfrak{F}\subset\mathfrak{A}$, consisting of all finite subsets of H, has order (or cardinal number) m, and it follows that a group isomorphic to $\mathfrak{F}$ may be defined on the elements of H.

11. Generalized quasigroup algebras. Let $\mathfrak{B}$ be a linear vector space of finite or infinite order over a field F. If Q is a quasigroup of finite or infinite order, let there be defined a linear algebra $\mathfrak{B}_{p,q}$ over F corresponding to any ordered pair p, q of elements of Q. Here $\mathfrak{B}_{p,q}$ consists of the vectors x, y of $\mathfrak{B}$ under the multiplication $(xy)_{p,q}$. Consider the linear set $\mathfrak{A}$ consisting of the elements

$$X = \sum x_p u_p, \qquad p \subset Q, \tag{11.1}$$

where the entities u_p are left-independent over $\mathfrak{B}$ and where the x_p are elements of $\mathfrak{B}$, only a finite number of them (unless otherwise stated) being distinct from the zero vector 0. We make $\mathfrak{A}$ into a linear algebra by defining the multiplication $X \cdot Y$ by the two-sided distributive law plus the definition

$$xu_p \cdot yu_q = (xy)_{p,q} \cdot u_{pq}. \tag{11.2}$$

Then $\mathfrak{A} = (\mathfrak{B}, Q)$ is called a *generalized quasigroup algebra* formed by extending the linear vector space $\mathfrak{B}$ by a quasigroup Q.

The analogy with quasigroup extensions should be plain. A necessary (but not in general sufficient) condition that $\mathfrak{A}$ be a division algebra is that each of the algebras $\mathfrak{B}_{p,q}$ be a division algebra. Thus although a division algebra is simply a linear algebra whose nonzero elements form a quasigroup under multiplication, the extension problem for division algebras is considerably complicated by linearity. We also note that if $\mathfrak{B} = F$ is simply the underlying field, and if $\mathfrak{B}_{p,q} = F$ for each pair p, q, then $\mathfrak{A} = (\mathfrak{B}, Q)$ is a quasigroup algebra in accordance with the definition of §6.

12. **Division rings of infinite order over a field.** If F is any field, consider the set of all formal power series

$$f(x) = \sum a_n x^n \tag{12.1}$$

in an indeterminate x, where the coefficients a_n are in F. If we assume that at most a finite number of the coëfficients a_n are nonzero for negative values of n, we may verify without difficulty that the set $N = (F, x)$ of all such power series forms a field of infinite order over F, where multiplication of power series is performed in the usual manner. David Hilbert has constructed an associative noncommutative division ring $\mathfrak{H} = (N, Z)$ of infinite order over F, by using an associative cross-product of the field N with the infinite cyclic group $Z = (y)$ [15, pp. 107–109 or 16, pp. 103–106]. Such a ring we shall call a *Hilbert division ring*. It is our purpose to define a *generalized Hilbert division ring* $\mathfrak{A} = (N, Z)$ by suitably adapting the suggestions of §11, that is, by constructing a "generalized group ring." We shall find it convenient to begin with some definitions and the proof of a simple lemma.

Definitions. (1) If $f(x)$, $g(x)$ are two elements of N, we designate by $fg(x)$ the element $f[g(x)]$, provided the latter exists in N after formal substitution and rearrangement[3].

(2) We call $\lambda(x) \subset N$ a *birational function* of x if (i) there exists a unique

[3] Note that if $f(x)$ is the formal expansion of $(1-x)^{-1}$ and if $g(x) = a + x$ for $a \neq 0$, then $fg(x)$ will not in general exist in the sense here defined.

element $\lambda^{-1}(x)$ of N such that $\lambda\lambda^{-1}(x)=\lambda^{-1}\lambda(x)=x$ and (ii) $f\lambda(x)$ and $f\lambda^{-1}(x)$ exist in N for every $f(x)\subset N$[4].

(3) If $\rho(x)$ is a birational function of x, we define the mth *iterate* $\rho^m(x)$ of $\rho(x)$ as follows, for m a positive or negative integer or zero:

$$\begin{aligned} \rho^0(x) &= x, & \rho^1(x) &= \rho(x), \\ \rho^{n+1}(x) &= \rho\rho^n(x), & \rho^{-n-1}(x) &= \rho^{-1}\rho^{-n}(x), \end{aligned} \tag{12.2}$$

where $n=1, 2, 3, \cdots$.

LEMMA 12A. *Let $\lambda(x)$, $\mu(x)$ be two birational functions of x. Then if $f(x)$, $h(x)$ are known elements of N, with $f(x)\neq 0$, there exists a unique $g(x)\subset N$ such that*

$$f\lambda(x)\cdot g\mu(x) = h(x), \tag{12.3}$$

namely

$$g(x) = h\mu^{-1}(x)/f\lambda\mu^{-1}(x). \tag{12.4}$$

Proof. The proof follows immediately if we replace x by $\mu^{-1}(x)$ in (12.3).

We obtain our "generalized group ring" $\mathfrak{A}=(N, Z)$ by suitably defining the product of two elements of the form

$$P = \sum f_m(x)y^m, \qquad Q = \sum g_n(x)y^n. \tag{12.5}$$

Here the $f_m(x)$, $g_n(x)$ are elements of N, and it is assumed that at most a finite number of the $f_m(x)$, $g_m(x)$ are nonzero for negative values of m. Let $\{\lambda_{m,n}(x)\}$, $\{\mu_{m,n}(x)\}$ be two arbitrary sets of birational functions of x, a pair $\lambda_{m,n}(x)$, $\mu_{m,n}(x)$ of such functions corresponding to every ordered pair m, n of integers, positive, negative, or zero. Then we define

$$f(x)y^m\cdot g(x)y^n = h(x)y^{m+n}, \tag{12.6}$$

where

$$h(x) = f\lambda_{m,n}(x)\cdot g\mu_{m,n}(x). \tag{12.7}$$

THEOREM 12A. *The ring $\mathfrak{A}=(N, Z)$, consisting of all elements P, Q given by* (12.5) *under the multiplication defined by* (12.6), (12.7), *is a division ring.*

Proof. We are required to prove that if in an equation

$$PQ = R = \sum h_p(x)y^p, \tag{12.8}$$

[4] Functions such as $\lambda(x)\equiv\lambda\cdot x$, where λ is a nonzero element of F, will be birational under the above definition, but it is doubtful whether there will exist more general birational functions. Suppose however that we replace the field $N=(F, x)$ of the present section by the field $F(x)$ consisting of all rational functions of the indeterminate x. Then $fg(x)$ will be defined in $F(x)$ for all $f(x)$, $g(x)$ of $F(x)$, and $\lambda(x)$ will be birational in $F(x)$ if and only if it is a quotient, not lying in F, of two linear functions [17, p. 181]. All results of this section will be valid whether $N=(F, x)$ or $N=F(x)$.

R is a given element of $\mathfrak{A}$, and one of P, Q is a given nonzero element of $\mathfrak{A}$, the third element is uniquely determined as an element of $\mathfrak{A}$. Since the proof is very similar in the two cases, we shall merely consider the case that $P\neq 0$ is a given element of $\mathfrak{A}$, and solve for Q.

We define the *degree* of a nonzero element P of $\mathfrak{A}$, given by (12.5), to be the least m such that $f_m(x)$ is not zero. It is clear that if $P\neq 0$ has degree u and $Q\neq 0$ has degree v then PQ has degree $u+v$. Hence if $R=0$, $P\neq 0$ in (12.8), the only solution for Q is $Q=0$. Therefore assume that P, R have respective degrees u, w. If Q exists it must have degree $v=w-u$. But then, using (12.5) and (12.8), we obtain an infinite series of equations for the coefficients $g_m(x)$ of Q, of which we write down the first two:

$$f_u\lambda_{u,v}(x)\cdot g_v\mu_{u,v}(x) = h_w(x),$$

$$f_u\lambda_{u,v+1}(x)\cdot g_{v+1}\mu_{u,v+1}(x) + f_{u+1}\lambda_{u+1,v}(x)\cdot g_v\mu_{u+1,v}(x) = h_{w+1}(x).$$

By virtue of Lemma 12A, $g_v(x)$ may be determined uniquely from the first equation. Then the only unknown in the second equation is $g_{v+1}(x)$, and this may be determined uniquely in the same manner. Clearly $g_{v+2}(x)$, $g_{v+3}(x)$, $\cdots$ may be uniquely determined, step by step, from subsequent equations, and hence Q exists and is unique.

In the special case that

$$\lambda_{m,n}(x) = x, \qquad \mu_{m,n}(x) = \rho^m(x), \tag{12.9}$$

for a fixed birational function $\rho(x)$ and for all m, n, we shall call $\mathfrak{A}=(N, Z)$ a Hilbert division ring. (In Hilbert's original example, $\rho(x)$ had the form $\rho(x)=2x$.)

LEMMA 12B. *Every Hilbert division ring is associative, but is commutative only in the case that* $\rho(x)=x$.

We leave it to the reader to show that, on the assumption of (12.9), we have

$$\begin{aligned}[f(x)y^m\cdot g(x)y^n]\cdot h(x)y^p &= f(x)y^m\cdot [g(x)y^n\cdot h(x)y^p] \\ &= [f(x)\cdot g\rho^m(x)\cdot h\rho^{m+n}(x)]\cdot y^{m+n+p}\end{aligned} \tag{12.10}$$

and

$$\begin{aligned} f(x)y^m\cdot g(x)y^n &= [f(x)\cdot g\rho^m(x)]\cdot y^{m+n}, \\ g(x)y^n\cdot f(x)y^m &= [g(x)\cdot f\rho^n(x)]\cdot y^{m+n}.\end{aligned} \tag{12.11}$$

From (12.10) the proof of associativity follows immediately. Again, if $\rho(x)=x$, it is evident that the two expressions of (12.11) will be identical, while if we assume their identity in the special case that $f(x)=1$, $g(x)=x$ we get $\rho^m(x)=x$ for all m or $\rho(x)=x$.

THEOREM 12B. *Let* $\mathfrak{A} = (N, Z, \lambda_{m,n}, \mu_{m,n})$ *be a generalized Hilbert division ring. Then*

(i) *necessary and sufficient conditions that* $\mathfrak{A}$ *have a unit element are*

$$\lambda_{m,0}(x) = \mu_{0,m}(x) = x \tag{12.12}$$

for all m. If conditions (12.12) *are satisfied,* $\mathfrak{A}$ *has unit element* y^0. *In any case* $\mathfrak{A}$ *is isotopic to a generalized Hilbert ring with unit element* y^0.

(ii) *Necessary and sufficient conditions that* $\mathfrak{A}$ *be commutative are*

$$\lambda_{m,n}(x) = \mu_{n,m}(x) \tag{12.13}$$

for all m, n.

(iii) *Necessary and sufficient conditions that* $\mathfrak{A}$ *be associative are the existence of a birational function* $\rho(x)$ *and a set of birational functions* $\lambda_n(x)$*such that*

$$\lambda_{m,n}(x) = \overset{-1}{\lambda_m}\lambda_{m+n}(x), \qquad \mu_{m,n}(x) = \overset{-1}{\lambda_n}\overset{m}{\rho}\lambda_{m+n}(x), \tag{12.14}$$

for all m, n. If conditions (12.14) *are satisfied* $\mathfrak{A}$ *is isomorphic to the Hilbert ring defined by* (12.9).

(iv) $\mathfrak{A}$ *is an alternative division ring if and only if it is associative.*

Remarks. From the various conditions displayed in Theorem 12B it should be clear that we may define non-associative division rings, commutative or noncommutative, and with or without a unit element. The associative law implies of course the existence of a unit element, and it is evident that equations (12.14) imply equations (12.12). An alternative division ring, by definition, is one whose nonzero elements form a Moufang quasigroup [4, §9] under multiplication, or possess a unique unit element and satisfy the law

$$P\cdot(Q\cdot RQ) = (PQ\cdot R)Q \tag{12.15}$$

for all elements P, Q, R. Since alternative rings occupy, so to speak, a midway position between associative and non-associative rings (see the above reference) it is perhaps a little disappointing to find that the generalized Hilbert rings offer only trivial examples.

The remainder of this section will be devoted to the proof of Theorem 12B.

(i) If $PQ = P \neq 0$, then Q must have degree 0. Assuming the special form $P = f_u(x)y^u \neq 0$ for P, we obtain

$$f_u\lambda_{u,0}(x)\cdot g_0\mu_{u,0}(x) = f_u(x),$$
$$f_u\lambda_{u,1}(x)\cdot g_1\mu_{u,1}(x) = 0,$$

and so on, whence we have $g_n(x) = 0$ for $n > 0$, and

$$g_0(x) = f_u\overset{-1}{\mu}_{u,0}(x)/f_u\lambda_{u,0}\overset{-1}{\mu}_{u,0}(x). \tag{12.16}$$

But if Q is to be independent of P, we find from (12.16) with $f_u(x) = 1$, $g_0(x) = 1$, and from (12.16) with $f_u(x) = x^{-1}$, $g_0(x) = \lambda_{u,0}\overset{-1}{\mu}_{u,0}(x)/\overset{-1}{\mu}_{u,0}(x)$. If these two values are to be identical we must have $\lambda_{u,0}\mu_{u,0}^{-1}(x)=\mu_{u,0}^{-1}(x)$ or $\lambda_{u,0}(x)=x$. Thus a necessary condition that Q be a right unit is $\lambda_{m,0}(x)=x$ for all m. In this case it follows from (12.16) that $g_0(x)=1$ and $Q=1\cdot y^0=y^0$. Moreover the condition may readily be seen to be sufficient as well in order that y^0 should be a right unit. The second condition $\mu_{0,m}(x)=x$ may be shown to be both necessary and sufficient that y^0 be a left unit. Hence equations (12.12) are necessary and sufficient for the existence of a unit element, which must be y^0 if it exists.

In general we define the linear transformations U, V of $\mathfrak{A}$ by assuming, in addition to the property of linearity, the equations

$$[f(x)y^m]^U = f\lambda_{m,0}^{-1}(x)\cdot y^m,\qquad [g(x)y^n]^V = g\mu_{0,n}^{-1}(x)\cdot y^n. \tag{12.17}$$

From (12.17), (12.6) and (12.7) we derive

$$[f(x)y^m]^U\cdot[g(x)y^n]^V = [f\lambda_{m,0}^{-1}\lambda_{m,n}(x)\cdot g\mu_{0,n}^{-1}\mu_{m,n}(x)]\cdot y^{m+n}.$$

Hence if $\mathfrak{A}_o$ be defined by $PoQ=P^U\cdot Q^V$, it is easy to see, first, that $\mathfrak{A}_o$ is a generalized Hilbert ring, and second, that $\mathfrak{A}_o$ has unit element y^0.

(ii) We shall have $PQ=QP$ for all elements of $\mathfrak{A}$ if and only if

$$f(x)y^m\cdot g(x)y^n = g(x)y^n\cdot f(x)y^m$$

for all m, n and all elements $f(x)$, $g(x)$ of N. This equation is equivalent to

$$f\lambda_{m,n}(x)\cdot g\mu_{m,n}(x) = g\lambda_{n,m}(x)\cdot f\mu_{n,m}(x). \tag{12.18}$$

From (12.18) with $f(x)=x$, $g(x)=1$ we derive equations (12.13); but conversely, if (12.13) holds true for all m, n then (12.18) will be satisfied for all m, n and all $f(x)$, $g(x)$ of N.

(iii) *and* (iv) Since the equations (12.15) are clearly satisfied in an associative algebra, we shall show that the assumption of (12.15) leads to (12.14). Assuming for the moment that equations (12.14) hold true in $\mathfrak{A}$, let us define the linear transformation T by

$$[f(x)y^m]^T = f\lambda_m(x)\cdot y^m, \tag{12.19}$$

so that

$$[f(x)\cdot y^m]^{T^{-1}} = f\lambda_m^{-1}(x)\cdot y^m. \tag{12.20}$$

Then, using (12.14), we readily find that

$$\{[f(x)y^m]^T\cdot[g(x)y^n]^T\}^{T^{-1}} = [f(x)\cdot g\rho^m(x)]\cdot y^{m+n}.$$

Hence the ring $\mathfrak{A}_o$, isomorphic to $\mathfrak{A}$, defined by

$$PoQ = (P^T\cdot Q^T)^{T^{-1}}, \tag{12.21}$$

is a Hilbert ring.

We now investigate (12.15). We shall need the following lemma.

LEMMA 12C. *If for four fixed elements a, b, c, d of N we have $f(a)f(b) = f(c)f(d)$ for all elements $f(x)$ of N, then either* (I) $a=c$, $b=d$ *or* (II) $a=d$, $b=c$.

Proof. For $f(x)=x$ we get $ab=cd$, and for $f(x)=1+x$ we get in addition $a+b=c+d$. Hence each of the pairs a, b and c, d comprises all the roots of a quadratic equation $t^2-ut+v=0$ ($u=ab=cd$, $v=a+b=c+d$) with coefficients in N. The lemma follows.

In (12.15) let $P=y^p$, $Q=f(x)y^q$, $R=y^r$ where $f(x)$ is an arbitrary element of N. We derive

$$(12.22)\quad \begin{aligned} &f\lambda_{q,q+r}\mu_{p,2q+r}(x)\cdot f\mu_{r,q}\mu_{q,q+r}\mu_{p,2q+r}(x) \\ &\qquad = f\mu_{p,q}\lambda_{p+q,r}\lambda_{p+q+r,q}(x)\cdot f\mu_{p+q+r,q}(x). \end{aligned}$$

An application of Lemma 12C to (12.22) shows that one of the following sets of equations must be satisfied for all p, q, r:

$$(I)\quad \begin{aligned} &(1)\quad \lambda_{q,q+r}\mu_{p,2q+r}(x) = \mu_{p,q}\lambda_{p+q,r}\lambda_{p+q+r,q}(x), \\ &(2)\quad \mu_{r,q}\mu_{q,q+r}\mu_{p,2q+r}(x) = \mu_{p+q+r,q}(x). \end{aligned}$$

$$(II)\quad \begin{aligned} &(1)\quad \lambda_{q,q+r}\mu_{p,2q+r}(x) = \mu_{p+q+r,q}(x), \\ &(2)\quad \mu_{r,q}\mu_{q,q+r}\mu_{p,2q+r}(x) = \mu_{p,q}\lambda_{p+q,r}\lambda_{p+q+r,q}(x). \end{aligned}$$

Case I. In addition to the two equations of (I) we must assume the equations (12.12), which ensure that $\mathfrak{A}$ has a unit element. We define

$$(12.23)\qquad \lambda_p(x) = \lambda_{0,p}(x), \qquad \mu_p(x) = \mu_{p,0}(x),$$

so that, in view of (12.12), we have

$$(12.24)\qquad \lambda_0(x) = \mu_0(x) = x.$$

From (12.12), (12.23), and I(2) with $q=0$, there comes $\mu_r\mu_{p,r}(x)=\mu_{p+r}(x)$, or

$$(12.25)\qquad \mu_{p,q}(x) = \overset{-1}{\mu_q}\,\mu_{p+q}(x).$$

But it may readily be verified, conversely, that I(2) is automatically satisfied when $\mu_{p,q}(x)$ is given by (12.25). By substitution from (12.25) in I(1), we derive

$$(12.26)\qquad \lambda_{q,q+r}\overset{-1}{\mu}_{2q+r}\mu_{p+2q+r}(x) = \overset{-1}{\mu_q}\,\mu_{p+q}\lambda_{p+q,r}\lambda_{p+q+r,q}(x).$$

Let $q=0$ in (12.26) and use (12.12), (12.23), (12.24). Thus

$$\lambda_r\overset{-1}{\mu_r}\,\mu_{p+r}(x) = \mu_p\lambda_{p,r}(x)$$

or

$$(12.27)\qquad \lambda_{p,q}(x) = \overset{-1}{\mu_p}\,\lambda_q\overset{-1}{\mu_q}\,\mu_{p+q}(x).$$

Substitution from (12.27) in (12.26) yields

$$\mu_q^{-1}\lambda_{q+r}\mu_{q+r}^{-1}\mu_{2q+r}\mu_{2q+r}^{-1}\mu_{p+2q+r}(x) = \mu_q^{-1}\mu_{p+q}\mu_{p+q}^{-1}\lambda_r\mu_r^{-1}\mu_{p+q+r}\mu_{p+q+r}^{-1}\lambda_q\mu_q^{-1}\mu_{p+2q+r}(x)$$

or, when x is replaced by $\mu_{p+2q+r}^{-1}(x)$ and both sides are "multiplied" by μ_q,

$$(12.28) \qquad \lambda_{q+r}\mu_{q+r}^{-1}(x) = \lambda_r\mu_r^{-1}\lambda_q\mu_q^{-1}(x).$$

We now define

$$(12.29) \qquad \tau_p(x) = \mu_p\lambda_p^{-1}(x), \qquad \mu_p(x) = \tau_p\lambda_p(x).$$

From (12.29) we substitute for $\mu_p(x)$ in (12.28), and derive $\tau_{q+r}^{-1}(x) = \tau_r^{-1}\tau_q^{-1}(x)$, or

$$(12.30) \qquad \tau_{p+q}(x) = \tau_p\tau_q(x).$$

If $\rho(x) = \tau_1(x)$, we may use mathematical induction and (12.30) to obtain

$$(12.31) \qquad \tau_n(x) = \rho^n(x).$$

Thus (12.29) and (12.31) give

$$(12.32) \qquad \mu_p(x) = \rho^p\lambda_p(x),$$

and this combines with (12.25) and (12.27) to yield the desired equations (12.14), which we have already shown to define a ring isomorphic to an (associative) Hilbert ring.

Case II. We shall deal with this case more briefly, using the above notation wherever applicable. From II(1) with $q=0$ we derive

$$(12.33) \qquad \mu_{p,q}(x) = \lambda_q^{-1}\mu_{p+q}(x);$$

and substitution from (12.33) in II(1) readily yields

$$(12.34) \qquad \lambda_{p,q}(x) = \lambda_p^{-1}\lambda_{p+q}(x).$$

From (12.33) and (12.34) in II(2),

$$(12.35) \qquad \mu_{q+r}\lambda_{q+r}^{-1}\mu_{2q+r}\lambda_{2q+r}^{-1}\mu_{p+2q+r}\lambda_{p+2q+r}^{-1}(x) = \mu_{p+q}\lambda_{p+q}^{-1}(x).$$

Thus (12.29) gives

$$(12.36) \qquad \tau_{q+r}\tau_{2q+r}\tau_{p+2q+r}(x) = \tau_{p+q}(x).$$

From (12.36) with $r=-q$, we find $\tau_q\tau_{p+q}(x) = \tau_{p+q}(x)$ or $\tau_q(x) = x$. Thus we have

$$(12.37) \qquad \mu_p(x) = \lambda_p(x).$$

Finally, (12.33), (12.34) and (12.37) give the desired equations (12.14). This time, however, we have the special case in which $\rho(x) = x$.

13. **Other division rings of infinite order.** Let F be an arbitrary field, let $Z = (x)$ be the infinite cyclic group, and let (F, Z) be the ring consisting of all

formal power series $f(x)$ with coefficients in F. It is understood, as in §12, that at most a finite number of the coefficients of negative powers of x in $f(x)$ are different from zero. However, in the present case, multiplication in (F, Z) is to be determined by

$$x^i \cdot x^j = c_{i,j}x^{i+j}, \tag{13.1}$$

where the $c_{i,j}$ are nonzero elements of F, defined for all integers i, j whether positive, negative, or zero. The proof of the following theorem is similar to that of Theorem 12A, but simpler.

THEOREM 13A. *The infinite ring (F, Z), just defined, is a division ring for all choices of the nonzero elements $c_{i,j}$.*

It should be noted that in the proof of Theorem 13A the fact that F is a field need not be used. In fact, provided a little care is exercised, F may be replaced by any division ring R, not necessarily associative or commutative. For example, if multiplication in (R, Z) is defined by

$$ax^i \cdot bx^j = (a \cdot bc_{i,j})x^{i+j}, \tag{13.2}$$

the reader will experience little difficulty in showing that (R, Z) is a division ring. It follows that we can define, successively, division algebras (F, Z), (F, Z, Z), and so on.

The rings just considered are not so much generalizations of as variations upon the generalized Hilbert rings of §12. Nevertheless the generalized Hilbert rings may also be generalized. We merely introduce an arbitrary set of nonzero elements $c_{m,n}(x)$ of N, and replace equations (12.6) and (12.7) by

$$f(x)y^m \cdot g(x)y^n = [f\lambda_{m,n}(x) \cdot g\mu_{m,n}(x) \cdot c_{m,n}(x)] \cdot y^{m+n}. \tag{13.3}$$

The resulting ring is a division ring.

The remarks of this section should indicate a broad avenue of research, down which, however, we shall venture no farther in this paper.

14. **Isotopy of division algebras.** Let $\mathfrak{A}$, $\mathfrak{A}_o$ be isotopic algebras of finite order n (not necessarily division algebras), such that

$$xoy = (x^U \cdot y^V)^W, \tag{14.1}$$

for nonsingular transformations U, V, and W. If the matrices L_x, R_x, and M_x are defined for $\mathfrak{A}$, relative to some basis, by (4.1) and (4.6), and if L_x^o, R_x^o and M_x^o are defined similarly for $\mathfrak{A}_o$, it is readily shown that

$$\overset{o}{L}_x = VL_pW, \qquad \overset{o}{R}_x = UR_qW, \qquad \overset{o}{M}_x = UM_rV', \tag{14.2}$$

where

$$p = x^U, \qquad q = x^V, \qquad r = x^W. \tag{14.3}$$

In fact the first two relations were given by Albert [2] and have been used previously in this paper. By taking determinants in (14.2) we derive

$$(14.4) \qquad |L_x^o| = bc|L_p|, \qquad |R_x^o| = ac|R_q|, \qquad |M_x^o| = ab|M_r|$$

with $a=|U|$, $b=|V|$, $c=|W|$. Hence the n-ary n-ic $|L_x^o|$ is projectively equivalent to the form $|L_x|$, and similarly for the other corresponding pairs.

THEOREM 14A. *A necessary condition that two algebras $\mathfrak{A}_o$ and $\mathfrak{A}$ should be isotopic is that the three n-ary n-ic forms $|L_x^o|$, $|R_x^o|$, and $|M_x^o|$ should be projectively equivalent to the forms $|L_x|$, $|R_x|$, and $|M_x|$ respectively.*

COROLLARY. *If the three n-ary n-ic forms $|L_x|$, $|R_x|$, and $|M_x|$ associated with an algebra $\mathfrak{A}$ are not projectively equivalent to the respective forms associated with an algebra $\mathfrak{B}$, then $\mathfrak{A}$ and $\mathfrak{B}$ are not isotopic.*

The Corollary to Theorems 14A is often useful in showing readily that two algebras are non-isotopic. We shall use it in the following sections in connection with division algebras.

15. **Quasigroup division algebras over the field of reals.** Let Q be a finite quasigroup, and let $\mathfrak{A}$ be a quasigroup algebra defined in terms of Q over a field F. We shall make a few prefatory remarks in case Q and F are arbitrary, and then specialize F to be the field of all real numbers and Q to be a group of order 4 or 8.

It is convenient for our purpose to define two quasigroups Q_* and Q_o, consisting of the same elements $p, q, r, \cdots$ as Q, by stating that each of the three following equations implies the other two.

$$(15.1) \qquad pq = r, \qquad p = q * r, \qquad q = p o r.$$

If Q is a group, or, more generally, a loop with the inverse property, it is readily verified that $q*r = rq^{-1}$ and $por = p^{-1}r$. Hence in this case Q_o is isotopic to Q and Q_* is anti-isomorphic to an isotope of Q. In the still more special case that Q is a totally symmetric loop we have $q*r = qr$, $por = pr$; and hence Q_* and Q_o are identical with Q. This latter situation occurs for example when Q is a direct power of the two-group [4, §8, Lemma 10].

Let $\mathfrak{A}$ have basis elements u_p with p in Q, where

$$(15.2) \qquad u_p u_q = h_{p,q} u_{pq},$$

and the $h_{p,q}$ are nonzero elements of the underlying field F. Then, according to Theorem 4A and Lemma 4A, $\mathfrak{A}$ will be a division algebra if and only if the $h_{p,q}$ are chosen (if possible) so that one of the determinants $|L_x|$, $|R_x|$, $|M_x|$ is nonzero for all nonzero x. If

$$(15.3) \qquad x = \sum x_p u_p,$$

comparison of (15.2) and (15.3) with (4.1), (4.3), and (4.6) gives

$$(15.4) \qquad L_x = (a_{p,q} x_{p*q}), \qquad R_x = (b_{p,q} x_{poq}), \qquad M_x = (h_{p,q} x_{pq}),$$

where in each case p designates the row and q the column, and where

$$a_{p,q} = h_{p*q,p}, \qquad b_{p,q} = h_{p,poq}. \tag{15.5}$$

For example we may use (15.3), (15.2) and (15.1) in succession and obtain

$$u_p \cdot x = u_p \cdot \sum_r x_r u_r = \sum_r x_r h_{p,r} u_{pr} = \sum_q x_{poq} h_{p,poq} u_q.$$

(Here we have set $r = poq$, whence $pr = q$.) Thus if $b_{p,q}$ has its expression in (15.5) we see that R_x is given by (15.4).

It follows from (15.4) that instead of studying quasigroup algebras directly we might equally well study linear sets of matrices of the form

$$T_x = (c_{p,q} x_{pq}), \tag{15.6}$$

where the $c_{p,q}$ are undetermined nonzero elements of the underlying field F, and pq designates the product of p and q in some finite quasigroup Q. We would seek to determine the $c_{p,q}$ so that the determinant $|T_x|$, an n-ary n-ic form, vanished only for $x=0$. Then, by identifying T_x with one of L_x, L_x', R_x, R_x', M_x, M_x', we would be able to define a quasigroup division algebra.

We now let the underlying field be the field of all real numbers, let Q be a loop, and suppose that the $h_{p,q}$ have been chosen so that $\mathfrak{A}$ has unit element $u_1 = 1$, 1 being the unit of Q. If Q has an element p such that $p^2 = 1$, then $B = (1, u_p)$ is a subalgebra of $\mathfrak{A}$ of order 2. If $\mathfrak{A}$ is a division algebra, $\mathfrak{B}$ must be isomorphic with the field of complex numbers; but $u_p^2 = h_{p,p}$ and hence $h_{p,p}$ must be negative. Thus[5] we may replace u_p by αu_p where $\alpha^2 = -h_{p,p}$, and obtain $u_p^2 = -1$.

In what follows we have made no further specialization of the $h_{p,q}$ without explicit mention, but have altered the notation in a manner appropriate to the case under consideration.

(I) *When Q is the four-group.* If $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ are six nonzero real numbers, let multiplication in $\mathfrak{A} = (1, i, j, k)$ be defined by

$$\begin{array}{c|cccc} & 1 & i & j & k \\ \hline 1 & 1 & i & j & k \\ i & i & -1 & \gamma k & -\beta' j \\ j & j & -\gamma' k & -1 & \alpha i \\ k & k & \beta j & -\alpha' i & -1 \end{array} . \tag{15.7}$$

Then M_x has the form of the interior of the multiplication table (15.7) except that $1, i, j, k$ must be replaced by x_0, x_1, x_2, x_3. An easy calculation gives $|M_x| = -G(x)$, where

[5] As the referee has remarked, it would be sufficient at this point to assume merely that the underlying field was *real closed.* Moreover much, but not quite all, of what follows in this section would be valid for any *formally real* field. We leave it to the reader to avoid the (very few) pitfalls.

$$\begin{aligned}G(x) = {} & x_0^4 + \alpha\alpha' x_1^4 + \beta\beta' x_2^4 + \gamma\gamma' x_3^4 \\ & + (1 + \alpha\alpha')x_0^2x_1^2 + (1 + \beta\beta')x_0^2x_1^2 + (1 + \gamma\gamma')x_0^2x_3^2 \\ & + (3\gamma + \beta'\gamma')x_2^2x_3^2 + (\gamma\alpha + \gamma'\alpha')x_3^2x_1^2 + (\alpha\beta + \alpha'\beta')x_1^2x_2^2 \\ & + [f(\alpha, \beta, \gamma) - f(\alpha', \beta', \gamma')]x_0x_1x_2x_3,\end{aligned} \tag{15.8}$$

and where

$$f(u, v, w) = u + v + w - uvw. \tag{15.9}$$

It may be shown moreover that $|L_x|$ and $|R_x|$ are obtainable from $G(x)$ by use of the permutations $(\alpha\beta')(\beta\gamma')(\gamma\alpha')$ and $(\alpha'\beta)(\beta'\gamma)(\gamma'\alpha)$ respectively. Note as a consequence that $|R_x|$ may be obtained from $|L_x|$ by use of $(\alpha\alpha')(\beta\beta')(\gamma\gamma')$, and conversely.

THEOREM 15A. *A necessary condition that the algebra $\mathfrak{A}$ with multiplication table* (15.7), *considered over the field of all real numbers, should be a division algebra, is that the six nonzero constants $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ should have the same sign. This sign may be taken to be positive without loss of generality. If the six constants are positive, a sufficient* (*but not necessary*) *condition for a division algebra is that they satisfy the relation*

$$f(\alpha, \beta, \gamma) = f(\alpha', \beta', \gamma') \tag{15.10}$$

where f is given by (15.9).

Proof of Theorem 15A. If the six constants are positive and satisfy (15.10) it is clear from (15.8) that $-|M(x)| = G(x)$ is a sum of non-negative terms and can vanish only if $x = 0$. Thus $\mathfrak{A}$ is a division algebra.

Conversely, if we set $x_2 = x_3 = 0$ in (15.8) we find $G(x) = G(x_0, x_1) = (x_0^2 + x_1^2)(x_0^2 + \alpha\alpha' x_1^2)$. If this expression is to vanish for real x_0, x_1 only when $x_0 = x_1 = 0$, it follows that $\alpha\alpha'$ must be positive. Similarly $\beta\beta'$ and $\gamma\gamma'$ must be positive. Again, since $G(x_2, x_3) = (\beta x_2^2 + \gamma' x_3^2)(\beta' x_2^2 + \gamma x_3^2)$, we see that $\beta\gamma'$ and $\beta'\gamma$ must be positive, and so on. It follows that the six constants must have the same sign. If all are negative we may replace i, j, k by $-i, -j, -k$ in (15.7) and derive new constants all of which are positive.

Finally, if the six constants are positive we may set

$$G(x) = F(x_0^2, x_1^2, x_2^2, x_3^2) + \lambda x_0x_1x_2x_3 \tag{15.11}$$

where F is a quadratic form with positive coefficients and $\lambda = f(\alpha, \beta, \gamma) - f(\alpha', \beta', \gamma')$. We have to thank S. Ulam for an approach which shows that the equation (15.10), or $\lambda = 0$, is unnecessary for a division algebra. In fact, taking absolute values we have

$$|G(x)| \geqq |F| - |\lambda x_0x_1x_2x_3|.$$

If we let $N>0$ be the maximum of the absolute values of x_0, x_1, x_2, x_3, and suppose that each of $\alpha\alpha'$, $\beta\beta'$, $\gamma\gamma'$ is not less than 1, we have $|F|\geqq N^4$. But on the other hand, we have $|\lambda x_0x_1x_2x_3|\leqq|\lambda|N^4$. Hence if $|\lambda|<1$ we may be sure that $|G(x)|$ is greater than 0 for $x\neq 0$. But the condition $0<|\lambda|<1$ may be secured for example by setting $\alpha'=\beta'=\gamma'=\alpha=1$, $\beta=1+h$, $\gamma=1+k$ with $h>0$, $k>0$ and $hk<1$. In fact we shall then have min $(\alpha\alpha',\beta\beta',\gamma\gamma')=1$, and also $\lambda=f(\alpha,\beta,\gamma)-f(\alpha',\beta',\gamma')=-hk$, $0<|\lambda|<1$. However, although λ need not be zero, it must submit to some restrictions. In fact, if $\alpha=\beta=\gamma$ and $\alpha'=\beta'=\gamma'$, we see from (15.8) with $x_0=x_1=x_2=x_3=1$ that $\mathfrak{A}$ will not be a division algebra if

$$4+6\alpha\alpha'+3\alpha^2+3\alpha'^2+3\alpha-\alpha^3-3\alpha'+\alpha'^3=0,$$

or if

$$u^3-6uv-(v^3+8)=0, \tag{15.12}$$

where

$$\alpha=\beta=\gamma=u+1, \qquad \alpha'=\beta'=\gamma'=v-1, \tag{15.13}$$

with $u>-1$, $v>1$. Thus from (15.12) we see that for every $v>1$ there exists a positive value u such that $\mathfrak{A}$ is not a division algebra under the assumption (15.13), even though the six constants α, β, γ, α', β', γ' are positive.

From this point on we shall suppose that the six constants are positive and satisfy (15.10). In case the equations

$$\alpha'=\alpha, \qquad \beta'=\beta, \qquad \gamma'=\gamma \tag{15.14}$$

are satisfied, the algebra (15.7) is one of the division algebras of rank 2 studied by L. E. Dickson [18, §4]. (For the definition of left rank and right rank of an algebra see [2, p. 694].)

THEOREM 15B. *A necessary and sufficient condition that the division algebra* (15.7) *should have two-sided rank* 2 *is that the equations* (15.14) *hold true. In the contrary case, the algebra has two-sided rank* 4.

Proof. If equations (15.14) are satisfied, we readily find from (15.7) that

$$x^2-2x_0x+N(x)=0, \qquad N(x)=x_0^2+x_1^2+x_2^2+x_3^2. \tag{15.15}$$

It follows that the algebra has two-sided rank 2. In the contrary case we may assume that $\gamma-\gamma'=\delta\neq 0$, and consider the element $a=i+j$. Then $a^2=-2+\delta k$, $a^2\cdot a=-2-\alpha'\delta i+\beta\delta j$, and the determinant of the coefficients of the four elements $1, a, a^2, a^2\cdot a$ reduces to $-(\alpha'+\beta)\cdot\delta\neq 0$. Hence a has right rank 4, and similarly a has left rank 4.

When (15.14) holds true it may be shown, by applying the permutation $(\alpha\beta')(\beta\gamma')(\gamma\alpha')$ to $G(x)$ and then using (15.14), that $|L_x|$ and $|R_x|$ both reduce to the product of the quadratic form $N(x)$ given in (15.15) by the quadratic form $x_0^2+\beta\gamma x_1^2+\gamma\alpha x_2^2+\alpha\beta x_3^2$. We state without proof the following easily derived lemma.

LEMMA 15A. *Necessary and sufficient conditions that the quaternary quartic form $G(x)$ given by* (15.8) *and* (15.10) *should reduce to a product of two quadratic forms are that the constants α, β, γ, α', β', γ' satisfy either the set of equations*

$$(\alpha-\beta')(\beta-\alpha') = (\beta-\gamma')(\gamma-\beta') = (\gamma-\alpha')(\alpha-\gamma') = 0 \tag{15.16}$$

or one of three sets of equations of which the following is typical:

$$(\alpha-\beta')(\beta-\alpha') = (\beta\gamma-1)(\beta'\gamma'-1) = (\gamma\alpha-1)(\gamma'\alpha'-1) = 0. \tag{15.17}$$

First we note that if the algebra has rank 2, so that (15.14) applies, then $|M_x| = -G(x)$ splits into quadratic factors, as does $|L_x| = |R_x|$, only if $\alpha=\beta=\gamma$ or $\alpha=\beta=\gamma^{-1}$, and so on. In the general case we may obtain the conditions that $|L_x|$ should split by applying to (15.16) and (15.17) and to the two sets of equations which we omitted the permutation $(\alpha\beta')(\beta\gamma')(\gamma\alpha')$; and in similar fashion we may derive the conditions for the splitting of $|R_x|$. It should be clear that we can choose positive numbers α, β, γ, α', β', γ', subject to the equation (15.10), such that none of $|L_x|$, $|R_x|$ and $|M_x|$ splits into quadratic factors; we must merely pick the six numbers distinct from each other and from their six inverses. For example the choice $\alpha=1$, $\beta=2$, $\gamma=51$, $\alpha'=3$, $\beta'=4$, $\gamma'=5$ has this property. It follows from Theorem 14A and Dickson's work on algebras of rank 2 that *the corresponding algebra $\mathfrak{A}$ is not isotopic to an algebra of rank* 2, and, even more, that *none of the five other division algebras associated with $\mathfrak{A}$ in the sense of* §4 *is isotopic to an algebra of rank* 2.

(II) *When Q is the cyclic group of order four.* If α, β, γ, α', β', γ', λ, λ' are 8 real nonzero constants, let multiplication in $\mathfrak{A}=(1, i, j, k)$ be defined by

$$\begin{array}{c|cccc} & 1 & i & j & k \\ \hline 1 & 1 & i & j & k \\ i & i & -1 & \gamma k & -\beta' j \\ j & j & -\gamma' k & \alpha i & \lambda \\ k & k & \beta j & -\lambda' & \alpha' i \end{array} . \tag{15.18}$$

This time we find $|M_x| = -G(x)$ where

$$\begin{aligned} G(x) = {} & \lambda\lambda' x_0^4 + \alpha\alpha' x_1^4 + \beta\beta' x_2^4 + \gamma\gamma' x_3^4 \\ & + (\lambda\lambda' + \alpha\alpha') x_0^2 x_1^2 + (\beta\gamma + \beta'\gamma') x_2^2 x_3^2 \\ & + x_2 x_3 \{ [\lambda(1-\beta\gamma) - \lambda'(1-\beta'\gamma')] x_0^2 + [\alpha(\beta'-\beta) + \alpha'(\gamma'-\gamma)] x_1^2 \} \\ & + x_0 x_1 \{ [\lambda\beta + \lambda'\beta' - \alpha\beta\beta' - \alpha'] x_2^2 + [\lambda\gamma + \lambda'\gamma' - \alpha'\gamma\gamma' - \alpha] x_3^2 \} . \end{aligned} \tag{15.19}$$

The quaternary forms $|L_x|$ and $|R_x|$ may be derived from $G(x)$ by substitutions on the eight constants, but it will be found simpler to calculate $|L_x|$ directly and to obtain $|R_x|$ from it (rather than from $G(x)$) by use of the substitution $(\lambda\lambda')(\beta\beta')(\gamma\gamma')$. We shall not go into detail in connection with the present division algebra, except to point out that it is unnecessary to make the terms in x_2x_3 and x_0x_1 vanish. For example, in the special case that

$$(15.20) \qquad \beta = \beta' = \gamma = \gamma' = 1, \qquad \lambda' = \lambda, \qquad \alpha' = \alpha, \qquad \lambda\alpha > 0,$$

$G(x)$ turns out to be the positive definite form

$$(15.21) \qquad G(x) = [\lambda x_0^2 + \alpha x_1^2]^2 + [(\lambda - \alpha)x_0x_1 + x_2^2 + x_3^2]^2.$$

It is interesting to note that when (15.20) holds we have

$$(15.22) \qquad |L_x| = |R_x| = (x_0^2 + x_1^2)^2 + \lambda\alpha(x_2^2 + x_3^2)^2.$$

Finally we remark that, irrespective of the choice of the eight nonzero constants, the algebra has two-sided rank 4. In fact the element j has rank 4.

(III) *When Q is the eight-group.* (By the eight-group we mean the direct product of the two-group and the four-group.) When Q has order eight the expansion of $|M_x|$ will involve $8! = 40,320$ terms, as against $4! = 24$ terms in the preceding work, and hence this method is clearly impractical. However the author was able to reduce the work to a calculation of only 105 terms by introduction of a Pfaffian; and the method, which leads to a wide variety of new division algebras of order 8, seems to deserve a brief description. Since Q is the eight-group, every element p except the unit element 1 has order two, and hence we assume in (15.2) that

$$(15.23) \qquad h_{1,q} = h_{q,1} = 1, \qquad h_{p,p} = -1 \qquad (p \neq 1).$$

In addition let us assume that

$$(15.24) \qquad h_{p,q} = -h_{q,p} \qquad (p, q, 1 \neq),$$

for p, q distinct from each other and from the unit element. Now the matrix $M_x = (h_{p,q}x_{pq})$ has x_0 in place (1, 1) and $-x_0$ in place (p, p) for $p \neq 1$. Thus if we multiply each row except row 1 of M_x by -1 we derive a new matrix

$$(15.25) \qquad T_x = x_0I + S_x$$

where I is the unit matrix and S_x is a skew-symmetric matrix which does not contain the variable x_0. In fact it is clear that T_x has x_0 down the main diagonal and hence that S_x has zero down the main diagonal. If furthermore $S_x = (c_{p,q})$, we have $c_{1,p} = h_{1,p} = 1$ and $c_{p,1} = -h_{p,1} = -1$ for $p \neq 1$; also $c_{p,q} = -h_{p,q}$ and $c_{q,p} = -h_{q,p} = +h_{p,q} = -c_{p,q}$ for 1, p, q all distinct. Thus S_x is skew-symmetric. Moreover $|M_x| = -|T_x|$. Finally we note that

$$(15.26) \qquad |T_x| = x_0^8 + P_1x_0^6 + P_2x_0^4 + P_3x_0^2 + P_4,$$

where the P_i are non-negative polynomials in the x_p for $p\neq 1$. This follows from two facts: (a) the coefficient of each odd power of x_0 is a sum of skew-symmetric determinants of odd dimension, and hence is zero; (b) the coefficient of each even power of x_0 is a sum of skew-symmetric determinants of even dimension, and hence a sum of squares. For example, the coefficient $P_4=|S_x|$ is equal to the perfect square of a polynomial of degree 4, the so-called *Pfaffian* of S_x.

If $|T_x|=0$ it follows that $x_0=0$ and that $P_4=|S_x|=0$. Conversely, if the $h_{p,q}$ are so determined that P_4 vanishes only when each x_p is zero ($p\neq 1$), then our algebra will be a division algebra. Since $P_4=[\Gamma(x)]^2$ where $\Gamma(x)$ is the Pfaffian we merely study $\Gamma(x)$. But the Pfaffian of a skew-symmetric determinant of 8 rows and columns is known to contain only $7\cdot 5\cdot 3\cdot 1=105$ terms. After making a judicious choice of the form of the multiplication table for Q the author calculated $\Gamma(x)$, and found that it consisted of 7 terms of the form x_p^4, the coefficient of each of these containing a single monomial; of 21 terms of the form $x_p^2x_q^2$, each coefficient being a sum of two monomials in the $h_{p,q}$; and finally, of 7 terms of the form $x_px_qx_rx_s$, each coefficient containing 8 monomials. It was possiblc in a variety of ways to make the coefficients of the 7 terms of the last type vanish, while at the same time making all the other coefficients positive.

As a variation on this method we may put L_x in the form T_x. In fact, from (15.4), (15.5), (15.1), and the fact that Q is the eight-group we derive

$$a_{p,q} = h_{pq,p}. \tag{15.27}$$

Hence it follows from (15.23) that $a_{1,q}=1$, $a_{p,1}=-1$ for $p\neq 1$ and $a_{p,p}=h_{1,p}=1$ for $p\neq 1$. Thus L_x will have the form (15.25) provided only

$$h_{pq,p} = -h_{pq,q} \qquad (p,\ q,\ 1\neq). \tag{15.28}$$

Similarly R_x will have the form (15.25) provided only

$$h_{p,pq} = -h_{q,pq} \qquad (p,\ q,\ 1\neq). \tag{15.29}$$

Finally, if we insist that equations (15.23), (15.24), (15.28) and (15.29) hold simultaneously, the resulting division algebra has a high degree of symmetry. If the $h_{p,q}$ are taken to have values ± 1, a proper choice of signs gives the well known Cayley-Graves-Dickson division algebra; but if on the other hand the same choice of signs is used, it is not necessary to require $h_{p,q}=\pm 1$. (Certain conditions are still necessary, however.)

In the following section we shall employ more elegant methods to derive some special examples of the algebras here described. It should be clear that the method just described breaks down when Q is the sixteen-group; indeed the Pfaffian of a skew-symmetric matrix of 16 rows and columns contains more than one million products.

16. Division algebras as generalized quasigroup algebras.

THEOREM 16A. *Let K be a field of degree one or two over a field F. Denote the elements of K by $a, b, \cdots$, and let the conjugate and norm of a be $\bar{a}$ and $N(a)=a\bar{a}$ respectively, where in case $K=F$ we have simply $\bar{a}=a$, $N(a)=a^2$. Consider the algebra $\mathfrak{A}$ (a quasigroup extension of K by the four-group) consisting of elements*

$$x = a_0 + a_1 i + a_2 j + a_3 k, \qquad y = b_0 + b_1 i + b_2 j + b_3 k$$

under the multiplication

$$\begin{aligned} x\cdot y = {} & [a_0 b_0 - a_1\bar{b}_1 - a_2\bar{b}_2 - a_3\bar{b}_3] \\ & + [a_1\bar{b}_0 + a_0 b_1 + c(\bar{a}_2\bar{b}_3 - \bar{a}_3\bar{b}_2)]i \\ & + [a_2\bar{b}_0 + a_0 b_2 + c(\bar{a}_3\bar{b}_1 - \bar{a}_1\bar{b}_3)]j \\ & + [a_3\bar{b}_0 + a_0 b_3 + c(\bar{a}_1\bar{b}_2 - \bar{a}_2\bar{b}_1)]k, \end{aligned} \tag{16.1}$$

where c is a fixed nonzero element of K. To every x of $\mathfrak{A}$ corresponds a conjugate $x'=\bar{a}_0-a_1i-a_2j-a_3k$ and a norm

$$N(x) = xx' = N(a_0) + N(a_1) + N(a_2) + N(a_3). \tag{16.2}$$

Moreover $(xy)'=y'x'$, but $\mathfrak{A}$ is an alternative algebra if and only if $N(c)=1$. Finally, $\mathfrak{A}$ is a division algebra if and only if $N(x)=0$ implies $x=0$, which is the case for example when F is a real field.

The multiplication (16.1) should be compared with that given by Dickson in his first proof that Cayley's algebra of order 8 over the reals was a division algebra [19, pp. 72–73]. In Dickson's paper $c=1$, but his proof goes through unchanged for $N(c)=1$. Thus $\mathfrak{A}$ is a direct generalization of the Cayley-Dickson algebra provided K is a quadratic extension of F. When $K=F$, and F is the field of reals, $\mathfrak{A}$ may be obtained from the algebra of Theorem 15A by equating the six constants α, α', and so on of that theorem to a fixed nonzero constant c; for general F it is a special case of Dickson's division algebras of rank 2, order 4 [19, 18]. We prove the theorem only for K quadratic; some trifling changes are required when $K=F$.

Proof of Theorem 16A. When y is replaced by $x'=\bar{a}_0-a_1i-a_2j-a_3k$ in (16.1) it follows immediately that $xx'=a_0\bar{a}_0+a_1\bar{a}_1+a_2\bar{a}_2+a_3\bar{a}_3=N(a_0)+N(a_1)+N(a_2)+N(a_3)=N(x)$. We leave it to the reader to prove, by use of (16.1), that

$$(xy)' = y'x'. \tag{16.3}$$

Now the conditions for an alternative algebra, in the present connection, may be given as

$$xy\cdot y' = x\cdot yy', \qquad y\cdot y'x = yy'\cdot x, \tag{16.4}$$

for all x, y of $\mathfrak{A}$, and it is readily seen from (16.3) that the first equation of (16.4) implies the second. Using the first equation we see that $\mathfrak{A}$ will be an alternative algebra if and only if $RyRy' = N(y) \cdot I_8$ where I_8 is the 8-rowed identity matrix. If a, b are in K we define the two-rowed matrices R_b and J by $a^{R_b} = ab = ba$ and $a^J = \bar{a}$. (Note that $J^2 = I$, where I is the two-rowed identity matrix.) It follows from the equation $\overline{ab} = \bar{a}\bar{b}$ that

$$R_bJ = JR\bar{b}. \tag{16.5}$$

Again, from (16.1) we derive

$$R_y = \begin{pmatrix} R_{b_0}, & R_{b_1}, & R_{b_2}, & R_{b_3} \\ -R_{\bar{b}_1}, & R_{\bar{b}_0}, & -JR_{\bar{b}_3c}, & JR_{\bar{b}_2c} \\ -R_{\bar{b}_2}, & JR_{\bar{b}_3c}, & R_{\bar{b}_0}, & -JR_{\bar{b}_1c} \\ -R_{\bar{b}_3}, & -JR_{\bar{b}_2c}, & JR_{\bar{b}_1c}, & R_{\bar{b}_0} \end{pmatrix},$$

$$R_{y'} = \begin{pmatrix} R_{\bar{b}_0}, & -R_{b_1}, & -R_{b_2}, & -R_{b_3} \\ R_{\bar{b}_1}, & R_{b_0}, & JR_{\bar{b}_3c}, & -JR_{\bar{b}_2c} \\ R_{\bar{b}_2}, & -JR_{\bar{b}_3c}, & R_{b_0}, & JR_{\bar{b}_1c} \\ R_{\bar{b}_3}, & JR_{\bar{b}_2c}, & -JR_{\bar{b}_1c}, & R_{b_0} \end{pmatrix}, \tag{16.6}$$

where $R_{y'}$ may be obtained from R_y by replacing b_0 by $\bar{b}_0$, b_1 by $-b_1$, and so on. It should be noted that R_y is an 8-rowed matrix in the elements of F, so that $|R_y|$ is in F, $|R_y| = |R_{y'}|$. Our next step is to calculate $R_yR_{y'}$; this requires some simple manipulations such as the following:

$$(-JR_{\bar{b}_3c})(JR_{\bar{b}_1c}) = -J \cdot R_{\bar{b}_3c}J \cdot R_{\bar{b}_1c} = -J^2 \cdot R_{b_3\bar{c}}R_{\bar{\bar{b}}_1c} = -R_{b_3\bar{b}_1} \cdot N(c).$$

If we define

$$M(y) = N(b_0) + N(c)[N(b_1) + N(b_2) + N(b_3)], \tag{16.7}$$

$$\alpha = 1 - N(c), \tag{16.8}$$

then

$$R_yR_{y'} = \begin{pmatrix} N(y)I, & 0 \\ 0, & Sy \end{pmatrix}, \tag{16.9}$$

where I is the two-rowed identity matrix and

$$S_y = \begin{pmatrix} [M(y) + \alpha N(b_1)]I, & \alpha R_{\bar{b}_2b_1}, & \alpha R_{\bar{b}_3b_1} \\ \alpha R_{\bar{b}_1b_2}, & [M(y) + \alpha N(b_2)]I, & \alpha R_{\bar{b}_3b_2} \\ \alpha R_{\bar{b}_1b_3}, & \alpha R_{\bar{b}_2b_3}, & [M(y) + \alpha N(b_3)]I \end{pmatrix}. \tag{16.10}$$

We may think of S_y as a 3-rowed matrix with elements of the form R_a. Since $|R_f| = f^2$ for f in F, and since the mapping $R_a \to a$ is an isomorphism of the set of all matrices R_a upon K, it follows that the determinant of S_y is the square of the determinant obtained by replacing I by 1 and generally R_a by a in S_y. Thus S_y is the square of

$$[M(y)]^3 + \alpha[M(y)]^2[N(b_1) + N(b_2) + N(b_3)] = [M(y)]^2 \cdot N(y),$$

as we see by expanding in ascending powers of α and using (16.8), (16.7) and (16.2). Hence from (16.9),

$$| R_y | \cdot | R_{y'} | = [N(y)]^2 \cdot [M(y)]^4[N(y)]^2 = [M(y)N(y)]^4,$$

and

$$| R_y | = [M(y)N(y)]^2. \tag{16.11}$$

Since $M(y)$ is the norm of $Y = b_0 + cb_1 \cdot i + cb_2 \cdot j + cb_3 \cdot j$, it follows that $\mathfrak{A}$ is a division algebra if and only if $N(x) = 0$ implies $x = 0$. Finally we see from (16.9), (16.10) that a necessary condition that $R_y R_{y'} = N(y) I_8$ is $\alpha = 0$, or $N(c) = 1$; the sufficiency follows from (16.7). This completes the proof.

For convenience, let us denote by $\mathfrak{A}(c)$ the division algebra defined by (16.1) for K quadratic over F. The following theorem shows that if F is the field of all real numbers there is no restriction in taking c to be real.

THEOREM 16B. *A necessary condition that a division algebra $\mathfrak{A}(d)$ should be isotopic to $\mathfrak{A}(c)$ is that $d = uc$ where $N(u) = 1$. If, conversely, $d = uc$ where $N(u) = 1$, then $\mathfrak{A}(d)$ is isomorphic to $\mathfrak{A}(c)$.*

Proof. Since the form $|R_x|$ is a projective invariant of the algebra $\mathfrak{A}(c)$ (by Theorem 14A) it follows from (16.11) and (16.7) that a necessary condition for isotopy of $\mathfrak{A}(c)$ and $\mathfrak{A}(d)$ is $N(c) = N(d)$. In this case we set $u = d/c$ and get $N(u) = 1$, $d = uc$. If, conversely, $N(u) = u\bar{u} = 1$ we define the linear transformation T by

$$x^T = a_0 + (\bar{u}a_1)i + a_2 j + a_3 k, \tag{16.12}$$

and set

$$xoy = (x^T \cdot y^T)^{T^{-}} . \tag{16.13}$$

A simple calculation, which we omit, shows that xoy has the form (16.1) with c replaced by $uc = d$; for example, the coefficient of i becomes

$$u[\bar{u}a_1\bar{b}_0 + a_0\bar{u}b_1 + c(\bar{a}_2\bar{b}_3 - \bar{a}_3\bar{b}_2)],$$

which simplifies as stated. But it follows from (16.13) that the algebra with multiplication xoy is isomorphic to $\mathfrak{A}(c)$.

In Theorem 15A we obtained a new type of division algebra by generalizing Dickson's expression of the Cayley-Dickson algebra of order 8 as an extension of a quadratic field by the four-group. A much more famous form of the Cayley-Dickson algebra, given by Dickson first for the field of reals and then for fields of characteristic not two [10, p. 14; 20, pp. 158–159], is an extension of the (generalized) quaternions by the two-group. Recently A. A. Albert [21, p. 171] has extended the definition to fields of arbitrary characteristic. After a few preparatory remarks we shall give a broad generalization of these results in Theorems 16C, 16D.

Let $\mathfrak{A}$ be an alternative division algebra of finite order n over a field F. (Thus, the nonzero elements of $\mathfrak{A}$ form a Moufang quasigroup.) It is known that $\mathfrak{A}$, if it is associative, must be either the field F $(n=1)$, a quadratic field over F $(n=2)$, or the generalized quaternions $(n=4)$. (If $\mathfrak{A}$ is non-associative then $\mathfrak{A}$ is a generalized Cayley-Dickson algebra and $n=8$.) If the elements of $\mathfrak{A}$ are denoted by $p, q, P, Q, \cdots$ and the product in $\mathfrak{A}$ by pq, there exists an involution $p \rightarrow p' = p^J$ of $\mathfrak{A}$ such that the elements

$$(16.14) \qquad p + p', \qquad pp' = p'p = N(p)$$

are in F. ($N(p)$ we call the norm and p' the conjugate of p.) Moreover,

$$(16.15) \qquad (pq)' = q'p', \qquad pq\cdot q' = p\cdot qq', \qquad q'\cdot qp = q'q\cdot p.$$

In the theorem which follows we wish to consider other algebras with the same elements as $\mathfrak{A}$. First we have a fixed but unspecified division algebra $\mathfrak{A}_o$, with multiplication poq and in general without a unit element. Next, for every fixed element a of $\mathfrak{A}$ we consider an algebra $\mathfrak{A}(a)$ whose product operation (*) is defined in terms of those of $\mathfrak{A}$ and $\mathfrak{A}_o$:

$$(16.16) \qquad p * q = poq - N(a)pq.$$

Theorem 16C. *Let $\mathfrak{A}$ be an alternative division algebra (as explained above) of finite order $n(n=1, 2, 4)$ over a field F. Let $\mathfrak{B}$ be an extension of $\mathfrak{A}$ by the two-group, consisting of elements $p+Pe$, $q+Qe$ with p, P, q, Q in $\mathfrak{A}$, under the multiplication*

$$(16.17) \qquad (p + Pe)(q + Qe) = (pq + Q'oP) + (Qp + Pq')e,$$

where (o) denotes multiplication in the unspecified division algebra $\mathfrak{A}_o$ (in general without a unit element) and p' is the conjugate of p in $\mathfrak{A}$. Then a necessary and sufficient condition that the algebra $\mathfrak{B}$, of order $2n$ over F, should be a division algebra is that the algebra $\mathfrak{A}(a)$ with multiplication (16.16) *should be a division algebra for every fixed element a of $\mathfrak{A}$. The unit element of $\mathfrak{A}$ is the unit element of $\mathfrak{B}$.*

Corollary 1. *If T is a linear transformation of $\mathfrak{A}$, none of whose characteristic roots are norms of elements of $\mathfrak{A}$, then $\mathfrak{B}$ is a division algebra when $poq = (pq)^T$ or $poq = pq^T$ or $poq = p^Tq$.*

Corollary 2. *If F is a subfield of the field of reals, if $n=4$, and if $p\times q$ denotes multiplication in one of the algebras of Theorem* 15A, *where the three* *positive constants* α', β', γ' *are any permutation of the three arbitrary positive constants* α, β, γ, *then the definition*

$$poq = -c^2(p \times q), \tag{16.18}$$

for any fixed nonzero element c *of* F, *yields a division algebra* $\mathfrak{B}$ *of order* 8.

Note that the Cayley-Dickson algebra results when $poq=fpq$ for f in F.

Proof of Theorem 16C. It is only necessary for the proof to find necessary and sufficient conditions that $\mathfrak{B}$ have divisors of zero. If the product given by (16.17) vanishes we must have

$$pq + Q'oP = 0, \tag{16.19}$$

$$Qp + Pq' = 0. \tag{16.20}$$

First we note that if $p\neq 0$ but $P=0$, these equations reduce to $pq=0$, $Qp=0$. In this case $q=Q=0$, since $\mathfrak{A}$ is a division algebra. Again, if $p=0$, $P\neq 0$ then $Q'oP=0$ and $Pq'=0$. Since $\mathfrak{A}$ and $\mathfrak{A}_o$ are both division algebras we derive $Q'=0$, $q'=0$, or $q=Q=0$. Hence if $p+Pe$ is a left-hand divisor of zero we must have $p\neq 0$, $P\neq 0$. Similarly if $q+Qe$ is the corresponding right-hand divisor of zero we must have $q\neq 0$, $Q\neq 0$. For the next stage in our proof we employ equations (16.14) through (16.20) but do not assume that $\mathfrak{A}$ is associative. From (16.19) after multiplication on the right by q', and from (16.20) after multiplication on the left by Q', we derive

$$pN(q) + (Q'oP)q' = 0, \tag{16.21}$$

$$N(Q)p + Q'\cdot Pq' = 0. \tag{16.22}$$

Conversely we may obtain (16.19) from (16.21) (by right multiplicition by q and division by $N(q)$) and (16.20) from (16.22). Now if we multiply (16.22) by the quotient $N(q)/N(Q)$ and subtract the resulting equation from (16.21), we have

$$(Q'oP)q' - (N(q)/N(Q))\cdot(Q'\cdot Pq') = 0. \tag{16.23}$$

If there exist three nonzero elements q, Q, P of $\mathfrak{A}$ which satisfy (16.23) we may solve (16.21) or (16.22) for p and thus satisfy (16.19), (16.20). Hence a necessary and sufficient condition that $\mathfrak{B}$ be a division algebra is that (16.23) have no solution for q, Q, P all different from 0. This much is valid even if $\mathfrak{A}$ is the Cayley-Dickson division algebra of order 8. Now we assume the associativity of $\mathfrak{A}$ and may divide on the right side in (16.23) by the nonzero element q'. This gives the equivalent equation

$$Q'oP - (N(q)/N(Q))\cdot Q'\cdot P = 0. \tag{16.24}$$

We define $a\neq 0$ by $a=qQ^{-1}$, so that $q=aQ$ and $N(a)=N(q)/N(Q)$, and derive

$$Q'oP - N(a)Q'P = 0. \tag{16.25}$$

Again, $\mathfrak{B}$ has divisors of zero if and only if, for some nonzero a, the equation (16.25) has a nonzero solution for P, Q. The equation (16.25) corresponding to the excluded value $a=0$ is $Q'oP=0$, which implies that one of P, Q is zero. Hence it is unnecessary to assume $a\neq 0$. Since (16.25) is the same as $Q' * P=0$, as we see from (16.16), the theorem is proved.

Proof of Corollary 1. If $poq=(pq)^T$ then $p*q=(pq)^T-N(a)pq$. But if p, q are not equal to 0, $p*q$ can vanish only when $N(a)$ is a characteristic root of T and $pq=r$ is the corresponding characteristic "vector." Hence it is necessary and sufficient to assume that none of the characteristic roots of T are norms of elements of $\mathfrak{A}$. The cases $poq=pq^T$ and $poq=p^Tq$ can be handled similarly.

Proof of Corollary 2. The algebra $\mathfrak{A}$ itself is obtained from Theorem 15A by putting the six constants equal to 1. Suppose that in $\mathfrak{A}(\times)$, with multiplication $p\times q$, α', β', γ' are a permutation of α, β, γ, and set $poq=-c^2(p\times q)$. Then from (16.16) we find $p*q=-[c^2+N(a)]\cdot\{p,q\}$, where $\{p,q\}$, given by

$$\{p,q\} = (c^2(p\times q)+N(a)pq)/(c^2+N(a)), \tag{16.26}$$

defines the product of p and q in still another algebra of Theorem 15A. This time α, α', and so on, have been replaced by

$$A = (c^2\alpha+N(a))/(c^2+N(a)), \qquad A' = (c^2\alpha'+N(a))/(c^2+N(a)), \tag{16.27}$$

and so on. Also if 1 is the unit element of $\mathfrak{A}(\times)$ we have, for example, as may be seen from (16.26), that

$$\{p,1\} = \{1,p\} = p, \qquad \{i,i\} = -1.$$

The six constants A, A', and so on, are all positive, and A', B', C' form the same permutation of A, B, C as do α', β', γ' of α, β, γ. Thus in particular we have

$$A+B+C-ABC = A'+B'+C'-A'B'C', \tag{16.28}$$

which ensures that the algebra with product $\{p,q\}$ is a division algebra. Hence $p*q=-[c^2+N(a)]\cdot\{p,q\}$ can only vanish if one of p, q vanishes; $\mathfrak{A}(a)$ is a division algebra for every element a of $\mathfrak{A}$, and $\mathfrak{B}$ is a division algebra.

The proof of Theorem 16C can also be stated in terms of certain determinants, and we shall obtain one of these. First, however, we wish to note a possible variation on the theorem.

THEOREM 16D. *If in Theorem* 16C, $\mathfrak{B}$ *be replaced by the algebra of couples* (p, P), *with* p, P *in* $\mathfrak{A}$, *under any of the three multiplications which follow, the conclusions of the theorem remain valid.*

$$(p,P)\cdot(q,Q) = (-poq-Q'P, Qp+Pq'), \tag{16.29}$$

$$(p,P)\cdot(q,Q) = (pq-Q'P, -Qop+Pq'), \tag{16.30}$$

$$(p,P)\cdot(q,Q) = (pq-Q'P, Qp-Poq'). \tag{16.31}$$

Theorem 16D must be proved for each of the three cases, but in every case the proof is very similar to the proof for Theorem 16D. The choice of the notation (p, P) seems desirable since in general the algebras of Theorem 16D do not have a unit element. For example if (u, U) is a unit element of $\mathfrak{B}$ under multiplication (16.29) it may be shown that $(u, U)=(1, 0)$, where 1 is the unit of $\mathfrak{A}$, and that $1op=po1=-p$; but this is a definite restriction on $\mathfrak{A}_o$. If in any one of the three cases we pass to an isotope with a unit element, the law of multiplication becomes more complicated.

Referring to the algebra (16.17), let us write $y=q+Qe$, $y'=q'-Qe$, $x=p+Pe$, and define the transformations R_x, L_x of B and the transformations R_p, L_p, R_p^o, L_p^o of $\mathfrak{A}$ and $\mathfrak{A}_o$ by

$$(16.32) \qquad xy = y^{L_x} = x^{R_y}, \qquad pq = q^{L_p} = p^{R_q}, \qquad poq = q^{L_p^o} = pR_q^o\,.$$

Then from (16.17) we derive

$$(16.33) \qquad Ry = \begin{pmatrix} Rq, & L_Q \\ L^o_{Q'}, & R_{q'} \end{pmatrix}, \qquad Ry' = \begin{pmatrix} R_{q'}, & -L_Q \\ -L^o_{Q'}, & Rq \end{pmatrix}.$$

Hence

$$(16.34) \qquad R_yR_{y'} = \begin{pmatrix} A_y & 0 \\ C_y & B_y \end{pmatrix}$$

with

$$(16.35) \qquad \begin{gathered} A_y = N(q)I - L_QL^o_{Q'}, \qquad B_y = N(q)I - L^o_{Q'}L_Q, \\ C_y = L^o_{Q'}R_{q'} - R_{q'}L^o_{Q'}. \end{gathered}$$

Now if Q is not equal to 0 we have $B_y=L_QA_yL_Q^{-1}$ and $|B_y|=|A_y|$, the latter equation being true even when $Q=0$. Hence from (16.34) we find $|R_y|\cdot|R_{y'}|=|A_y|^2$, or

$$(16.36) \qquad |R_y| = |R_{y'}| = |N(q)I - L_QL^o_{Q'}|.$$

If either $poq=(pq)^T$ or $poq=pq^T$ we readily deduce that

$$|Ry| = |N(q)I - N(Q)T|,$$

from which it is clear that a necessary condition for the isotopy of two algebras of either of these forms is that the two T's in question have the same characteristic roots. Since the Cayley-Dickson algebra corresponds to $T=fI$, f in F, we have obtained an essential generalization.

Before leaving the algebras of Theorem 16C we wish to show that among them are algebras of right-rank and left-rank 8. For example, let $n=4$, F be the real field, $\mathfrak{A}=(1, i, j, k)$ be the real quaternions and $\mathfrak{A}_o$ be defined by $poq=(pq)^T$ where

$$(16.37)\qquad T = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Then $|T-\lambda I| = \lambda^4+1$, the characteristic roots of T are not norms of quaternions, $\mathfrak{B}$ is a division algebra of order 8. Moreover if $x=ie$, we use (16.17) and $poq=(pq)^T$ to obtain $x^2=(-i\cdot i)^T=1^T=-i$, $x^3\equiv x^2\cdot x=e$, $x^4\equiv x^3\cdot x=(-i\cdot 1)^T=j$, $x^5\equiv x^4\cdot x=ke$, $x^6\equiv x^5\cdot x=(-i\cdot k)^T=-k$, $x^7\equiv x^6\cdot x=je$, $x^8\equiv x^7\cdot x=(-i\cdot j)^T=-1$. Thus the right minimal equation of $x=ie$ is $\lambda^8+1=0$. It may be shown similarly that $\lambda^8+1=0$ is also the left minimal equation of x.

1 . **Some division algebras of order $2n$.** Some preliminary theory will be required. If $\mathfrak{A}$ is an arbitrary algebra of order n over a field F, let $\mathfrak{R}=(R_x)$ be the linear set of right mappings of $\mathfrak{A}$, and $\mathfrak{C}\subset M_n$ be the commutator algebra of $\mathfrak{R}$. Define the *left-associator* of $\mathfrak{A}$ to be the associative subalgebra $\mathfrak{S}\subset\mathfrak{A}$ consisting of all elements a of $\mathfrak{A}$ such that

$$(17.1)\qquad ax\cdot y = a\cdot xy$$

for all x, y of $\mathfrak{A}$.

LEMMA 17A. *If $\mathfrak{A}$ has a unit element e, the commutator algebra $\mathfrak{C}$ of $\mathfrak{R}=(R_x)$ is anti-isomorphic to the left associator $\mathfrak{S}$ of $\mathfrak{A}$.*

The lemma is sufficiently general for our purpose. However we shall actually prove that *a sufficient condition for $\mathfrak{C}$ to be anti-isomorphic to $\mathfrak{S}$ is that $\mathfrak{A}$ have a left unit e and at least one right nonsingular element r.* If C is in $\mathfrak{C}$, we have $CR_y=R_yC$ for every y of $\mathfrak{A}$, and hence

$$(17.2)\qquad x^C\cdot y = (xy)^C$$

for all x, y of $\mathfrak{A}$. If $\mathfrak{A}$ has left unit e we define $a=e^C$, set $x=e$ in (17.2), and obtain $ay=y^C$,

$$(17.3)\qquad C = L_a.$$

But substitution of $C=L_a$ in (17.2) yields (17.1), and conversely (17.1) and (17.3) imply (17.2). Moreover if a, b are elements of $\mathfrak{S}$ we have $ab\cdot y=a\cdot by$ for all y, or $L_{ab}=L_bL_a$. Thus if $\mathfrak{A}$ has a left unit e, the mapping $a\rightarrow L_a$ is an anti-homomorphism of $\mathfrak{S}$ upon $\mathfrak{C}$. In fact if $\mathfrak{N}$ is the left-annihilator of $\mathfrak{A}$, namely the set of elements $a\subset\mathfrak{A}$ such that $ax=0$ for all x, we have $\mathfrak{C}$ anti-isomorphic to $\mathfrak{S}/\mathfrak{N}$. A sufficient, but not necessary, condition that $\mathfrak{N}$ contain only the zero element is that $\mathfrak{A}$ have a right nonsingular r (we may take $r=e$ if e is a two-sided unit); and in case the condition holds $\mathfrak{C}$ is anti-isomorphic to $\mathfrak{S}$.

LEMMA 17B. *Let $\mathfrak{A}$ have order n, unit element e. If the commutator algebra $\mathfrak{C}$*

of $\mathfrak{R}$ has order $m \geqq n$ then $m = n$ and $\mathfrak{A}$ is an associative algebra anti-isomorphic to $\mathfrak{C} = \mathfrak{L} = (L_x)$.

According to Lemma 17A, $\mathfrak{C}$ is anti-isomorphic to $\mathfrak{S} \subset \mathfrak{A}$. Hence $m \leqq n \leqq m$, $m = n$, $\mathfrak{S} = \mathfrak{A}$, $\mathfrak{A}$ is associative, $\mathfrak{C} = \mathfrak{L} = (L_x)$.

Let $\mathfrak{V}$ be a linear vector space of order n over F, with elements $p, q, P, Q, \cdots$. Let $\mathfrak{A}(\cdot)$, $\mathfrak{A}(o)$, $\mathfrak{A}(\times)$, $\mathfrak{A}(*)$ be four arbitrary algebras defined on $\mathfrak{V}$, with multiplications denoted by $p \cdot q$, poq, $p \times q$, $p * q$ respectively. Then the most general extension $\mathfrak{B}$ of $\mathfrak{V}$ by the two-group is the set of all couples (p, P) under the multiplication

$$(17.4) \qquad (p, P) \cdot (q, Q) = (p \cdot q + PoQ, p \times Q + P * q).$$

If $\mathfrak{B}$ is a division algebra the four algebras $\mathfrak{A}$ are division algebras, and henceforth we shall assume the $\mathfrak{A}$'s to be division algebras, without however making any assumption as to their possession of right or left units. We define the transformations R_q, U_q, V_q, W_q of $\mathfrak{V}$ by

$$(17.5) \qquad pq = p^{R_q}, \qquad poq = p^{U_q}, \qquad p \times q = p^{V_q}, \qquad p * q = p^{W_q}.$$

If $x = (p, P)$, $y = (q, Q)$, and R_y is defined by $xy = x^{R_y}$, then from (17.4) follows

$$(17.6) \qquad R_y = \begin{pmatrix} R_q, & V_Q \\ U_Q, & W_q \end{pmatrix}.$$

Since the $\mathfrak{A}$'s are division algebras R_y is nonsingular for $q = 0$, $Q \neq 0$ and for $q \neq 0$, $Q = 0$. Assuming $q \neq 0$ we may multiply R_y on the left by the nonsingular matrix

$$\begin{pmatrix} I & 0 \\ -U_Q R_q^{-1}, & I \end{pmatrix}$$

and obtain a matrix with a zero matrix below the main diagonal and with the matrices R_q, $W_q - U_Q R_q^{-1} V_Q$ down the main diagonal. Hence *if the $\mathfrak{A}$'s are division algebras, a necessary and sufficient condition that the algebra $\mathfrak{B}$ with multiplication table* (17.4) *should be a division algebra is that the matrix $W_q - U_Q R_q^{-1} V_Q$ be nonsingular for q, $Q \neq 0$.* This test, or its counterpart for either of the matrices L_x and M_x, could be applied successfully to the algebras of Theorems 16C and D, but in itself it does not offer any suggestion as to judicious choices of the four $\mathfrak{A}$'s.

Let us change tactics and calculate the matrix $R_x R_y$ where $x = (p, P)$. From (17.6) we derive

$$(17.7) \qquad R_x R_y = \begin{pmatrix} R_p R_q + V_P U_Q, & R_p V_Q + V_P W_q \\ U_P R_q + W_q U_Q, & U_P V_Q + W_p W_q \end{pmatrix}.$$

Clearly $\mathfrak{B}$ will be a division algebra if and only if $R_x R_y$ is nonsingular for all x, $y \neq 0$. It is our purpose to investigate the type of algebra $\mathfrak{B}$ which results when one of the four matrix elements in the expression for R_xR_y vanishes for all $x\neq 0$ and suitably chosen $y\neq 0$. In each of the four possible cases the analysis can be carried through to a successful conclusion, but we shall consider only the case that

$$R_pV_Q + V_PW_q = 0 \tag{17.8}$$

for all $x=(p, P)$ and for some $y=(q, Q)\neq 0$ which will be seen to depend upon x. If $p=0$, $P\neq 0$ then (17.8) gives $V_PW_q=0$, $W_q=0$, $q=0$. Hence q vanishes whenever p vanishes. Similarly Q vanishes whenever P vanishes. Thus the simplest hypothesis which we can make concerning y is given by

$$y = x^T = (p^J, P^K) \tag{17.9}$$

where J, K are linear transformations which we shall take to be nonsingular. Then, if we make a convenient change in notation by replacing P by q, (17.9) and (17.8) imply

$$R_pV_{qK} + V_qW_{pJ} = 0, \tag{17.10}$$

for all p, q of $\mathfrak{B}$. Let A, B, C, D be four nonsingular linear transformations of $\mathfrak{B}$, and define nonsingular transformations θ, ϕ of B by

$$x = (p, P), \qquad x^\theta = (p^A, P^B), \qquad x^\phi = (p^C, P^D). \tag{17.11}$$

In terms of θ and ϕ we may define an algebra $\mathfrak{B}_o$ isotopic to $\mathfrak{B}$, where the multiplication $x\cdot y$ of (17.4) is replaced by

$$\begin{aligned} xoy &= (x^\theta\cdot y^\phi)^{\theta^{-1}} \\ &= ([p^A\cdot q^C]^{A^{-1}} + [P^BoQ^D]^{A^{-1}}, [p^A\times Q^D]^{B^{-1}} + [P^B * q^C]^{B^{-1}}). \end{aligned} \tag{17.12}$$

If we distinguish the new matrices corresponding to those of (17.5) by a superscript o, then

$$\begin{gathered} \overset{o}{R}_p = AR_{(p^C)}A^{-1}, \quad \overset{o}{U}_p = BU_{(p^D)}A^{-1}, \quad \overset{o}{V}_p = AV_{(p^D)}B^{-1}, \\ \overset{o}{W}_p = BW_{(p^C)}B^{-1}. \end{gathered} \tag{17.13}$$

If further we define

$$J_o = CJC^{-1}, \qquad K_0 = DKD^{-1}, \tag{17.14}$$

then by a computation which is complicated only in appearance we find that (17.10) implies

$$\overset{o}{R}_p\overset{o}{V}_{(qK_o)} + \overset{o}{V}_q\overset{o}{W}_{(pJ_o)} = 0. \tag{17.15}$$

In fact the expression on the left of (17.15) reduces to AMB^{-1} where M stands for the left side of (17.10) with p, q replaced by $p_o=p^C$, $q_o=q^D$ respectively. Hence *the property* (17.10) *of* $\mathfrak{B}$ *is invariant under the isotopic transformation defined by* (17.12).

As may be seen from (17.12), $\mathfrak{A}(\cdot)$ has been replaced by an algebra $\mathfrak{A}_o(\cdot)$ in which the ordered product of p and q is $(p^A \cdot q^C)^{A^{-1}}$, and $\mathfrak{A}(\times)$ by $\mathfrak{A}_o(\times)$ in which the product of p and q is $(p^A q^D)^{B^{-1}}$. Note that $\mathfrak{A}_o(\cdot)$ will have a right unit if and only if $\mathfrak{A}(\cdot)$ has a right unit. Again, if e is any specified element of $\mathfrak{B}$, the necessary and sufficient conditions that e be a left unit of $\mathfrak{A}_o(\cdot)$ and a two-sided unit of $\mathfrak{A}_o(\times)$ are easily seen to be

$$(17.16)\qquad (e^A \cdot p^C)^{A^{-1}} = (e^A \times p^D)^{B^{-1}} = (p^A \times e^D)^{B^{-1}} = p.$$

If the left multiplications L_p, T_p of $\mathfrak{A}(\cdot)$ and $\mathfrak{A}(\times)$ respectively be defined by

$$(17.17)\qquad p \cdot q = q^{L_p}, \qquad p \times q = q^{T_p},$$

we may state a lemma.

Lemma 17C. *Let f, g be arbitrary nonzero elements of $\mathfrak{B}$, and let the nonsingular transformation B be chosen so that $e^B = f \times g$. Then a solution of* (17.16) *is given by*

$$(17.18)\qquad A = BV_g^{-1}, \qquad C = BV_g^{-1}L_f^{-1}, \qquad D = BT_f^{-1},$$

and in fact every solution A, B, C, D has this form.

We remind the reader of Theorem 3D. It is not difficult to verify the fact that (17.18) yields a solution of (17.16), and the rest of the lemma is not essential for our purposes. From this point onward we assume that e is a left unit of $\mathfrak{A}(\cdot)$ and a two-sided unit of $\mathfrak{A}(\times)$. It follows that $u = (e, o)$ is a left unit of $\mathfrak{B}$ and that $V_e = I$.

From (17.10) with $q = e$,

$$(17.19)\qquad W_{pJ} = -R_p H, \quad \text{where} \quad H = V_a, \quad a = e^K.$$

Substitution from (17.19) in (17.10) gives

$$(17.20)\qquad R_p V_{(qK)} = V_q R_p H,$$

whence for $p = e$,

$$(17.21)\qquad V_{qK} = Z^{-1} V_q Z \cdot H, \qquad Z = R_e.$$

Thus from (17.20) and (17.21), $R_p Z^{-1} V_q Z H = V_q R_p H$, or

$$(17.22)\qquad R_p Z^{-1} \cdot V_q = V_q \cdot R_p Z^{-1}.$$

Since the V_q are right multiplications of an algebra $\mathfrak{A}(\times)$ with a unit element, we may apply Lemma 17B to show that $\mathfrak{A}(\times)$ is an *associative* algebra anti-isomorphic to the algebra $\mathfrak{T}$ consisting of all transformations T_r where $r = e^{R_p Z^{-1}} = (ep)^{Z^{-1}} = p^{Z^{-1}}$. Thus $R_p Z^{-1} = T_r$, or

$$(17.23)\qquad R_p = T_r Z, \qquad r = p^{Z^{-1}}, \qquad Z = R_e.$$

Moreover, (17.23) and (17.19) give

$$(17.24)\qquad W_p = -T_s ZH, \qquad s = p^{J^{-1}Z^{-1}}.$$

These last two equations allow us to write

$$(17.25)\qquad R_x = \begin{pmatrix} T_r Z, & V_P \\ U_P, & -T_s ZH \end{pmatrix}.$$

Since $u=(e, o)$ is a left unit of $\mathfrak{B}$ we may pass to the isotope $\mathfrak{B}_o$ defined by $xoy=x^{R_u^{-1}}\cdot y^{L_u^{-1}}=x^{R_u^{-1}}\cdot y$ and replace R_x by $R_x^o=R_u^{-1}R_x$. Now from (17.25), (17.23), and (17.24),

$$(17.26)\qquad R_u = \begin{pmatrix} Z, & 0 \\ 0, & -T_b ZH \end{pmatrix}, \qquad b = e^{J^{-1}Z^{-1}}.$$

Hence R_u^{-1} is diagonal and we may appropriately define T_o by setting $R^o_{(x^{T_o})}=R_{(x^T)}$, where T is given by (17.9). In this case $R_x^o R_{(x^{T_o})}=R_u^{-1}R_x R_{(x^T)}$; and therefore the property (17.10) is not destroyed. But we have now arranged that $u=(e, o)$ is a two-sided unit of $\mathfrak{B}$ and that $\mathfrak{B}$ has property (17.10). We have lost the property that e is a right unit of $\mathfrak{A}(\times)$, but can regain this property by a further use of (17.18) without having to relinquish the newly gained point that e is a right unit of $\mathfrak{A}(\cdot)$. Thus we may assume $Z=R_e=I$. From (17.23), $T_p=R_p$ and the associative algebra $\mathfrak{A}(\times)$ is anti-isomorphic to the associative algebra $\mathfrak{A}(\cdot)$,

$$(17.27)\qquad p\times q = q\cdot p, \qquad T_p = R_p, \qquad V_q = L_q.$$

From (17.21), $V_{(q^K)}=V_q H=V_q V_a$, or $L_{(q^K)}=L_q L_a=L_{aq}$, or

$$(17.28)\qquad q^K = aq, \qquad K = L_a.$$

From (17.19), $W_{p^J}=-R_p V_a=-R_p L_a$, and on replacing p by $q^{J^{-1}}$ and operating on p we get $p*q=-apq^{J^{-1}}$, or

$$(17.29)\qquad p*q = apq^{\lambda}, \qquad \lambda = -J^{-1}.$$

But $\mathfrak{A}(*)$ has right unit e, so that $ape^{\lambda}=p$, $ap=p(e^{\lambda})^{-1}$, $a=(e^{\lambda})^{-1}$ is in the centre of $\mathfrak{A}(\cdot)$,

$$(17.30)\qquad p*q = pq^{\theta}, \qquad \theta = -L_a J^{-1} = -J^{-1}R_a.$$

In particular we now have $e^{\theta}=e$, and

$$(17.31)\qquad x\cdot y = (p, P)\cdot(q, Q) = (p\cdot q + PoQ, Q\cdot p + P\cdot q^{\theta}).$$

It is convenient to change our definition of T, and we do so, defining

$$(17.32)\qquad x^T = (p, P)^T = (p^{\phi}, -P), \qquad \phi = \theta^{-1}.$$

THEOREM 17A. *Let algebra $\mathfrak{B}$, with multiplication table* (17.4), *the component algebras $\mathfrak{A}$ being division algebras of order n over F, have the property* (17.10) *for some T given by* (17.9). *Then $\mathfrak{B}$ may be replaced by a suitable isotope with a* *unit element* $u=(e, o)$ *such that* $e^\theta=e$. *The algebra* $\mathfrak{A}(\cdot)$ *is now an associative division algebra and* $\mathfrak{B}$ *has multiplication* (17.31). *Moreover* T *may be redefined to have form* (17.32); *and we derive*

$$(17.33)\qquad R_xR_{x^T}=\begin{pmatrix} R_pR_{p^\phi}-L_PU_P, & 0 \\ * & R_{p^\theta}R_p-U_PL_P \end{pmatrix}.$$

Thus $\mathfrak{B}$ *is a division algebra if and only if* $R_pR_{p^\phi}-L_PU_P$ *and* $R_pR_{p^\phi}-U_PL_P$ *are nonsingular for all* p, P.

Note that the mapping $p\rightarrow p^\theta$ sends $R_pR_{p^\phi}-U_PL_P$ into $R_{p^\theta}R_p-U_PL_P$, and hence that the one matrix is nonsingular for all x if and only if the other is. A like statement is true of the two matrices mentioned in the last sentence of Theorem 17A, since, for $P\neq 0$, the latter matrix may be obtained from the former by multiplying on the right and left respectively by the nonsingular matrix L_P and its inverse.

If the underlying field is the field of all real numbers, then $\mathfrak{A}=\mathfrak{A}(\cdot)$ is either the complex numbers or the quaternions. Thus if θ is an involution of $\mathfrak{A}$ such that $p+p^\theta$ and pp^θ are in F we have rediscovered the algebras of Theorem 16C. (By similar processes we may also obtain the algebras of Theorem 16D.)

In case $\mathfrak{A}$ is an extension field of degree n over F, suppose that $\mathfrak{A}$ is cyclic and let θ be a generator of the Galois group. Following L. E. Dickson [18, p. 123] we may take

$$(17.34)\qquad poq=fpq^\theta\cdot J$$

where $J, J^\theta, \cdots, J^{\theta^{n-1}}$ form a normal basis of $\mathfrak{A}$ and the nonzero numbers f and $N(J)=JJ^\theta\cdots J^{\theta^{n-1}}=c$ are in F. Then $U_q=fR_{(q^\theta J)}$, $L_p=R_p$, and

$$R_pR_{p^\phi}-L_PU_P=R_pR_{p^\phi}-U_PL_P=R_s$$

where

$$(17.35)\qquad s=pp^\phi-fJPP^\theta,\qquad \phi=\theta^{-1}=\theta^{n-1}.$$

Thus $\mathfrak{B}$ is a division algebra unless we can have $s=0$ for $x=(p, P)\neq 0$. If $n=2$, then $\phi=\theta$ and the quantity $s=N(p)-fN(P)J$ cannot vanish since J is not in F. For $n>2$ the equation $s=0$ implies $pp^{\theta^{n-1}}=fJPP^\theta$, and hence

$$\prod_{r=0}^{n-1}p^{\theta^r}p^{\theta^{r-1}}=f^n\cdot\prod_{r=0}^{n-1}J^{\theta^r}\cdot\prod_{r=0}P^{\theta^r}P^{\theta^{r-1}}$$

or $[N(p)]^2=f^nc\cdot[N(P)]^2$. Therefore if f^nc is not the square of a norm, $\mathfrak{B}$ is a division algebra. (This is precisely Dickson's proof.)

We have no further results on the algebras of Theorem 17A. In conclusion we wish to mention without proof the result of still another investigation on division algebras.

THEOREM 17B. *Let $G(\cdot)$ and $G(o)$ be two loops of finite order $m>1$ consisting of the same elements $p, q, \cdots$. Define $A_x=(a_{p,q}x_{p\cdot q})$, $B_x=(b_{p,q}x_{p\circ q})$, where the $a_{p,q}$, $b_{p,q}$ are real numbers and $x=(x_p)$ is a vector with real components. Assume that $A_xB_x=D_x$ where D_x is a diagonal matrix, nonsingular for $x\neq 0$, whose diagonal elements are definite forms in x (positive or negative definite). Then $m=2^n$ for $n=1$, 2 or 3, and $G(\cdot)=G(o)=G$, where G is the nth direct power of the two-group. Essentially the only solution of the problem is given by $A_x=R_x$, $B_x=R_{x'}$, $D_x=N(x)I$, where R_x is the right multiplication associated with an element x of an alternative algebra permitting composition* [21] *and x', $N(x)=xx'$ are respectively the conjugate and norm of x.*

I should not like to conclude this paper without some mention of an important omission from the bibliography of the companion paper [4] on quasigroups. In two papers [22] which appeared in the Transactions, R. Baer has given an interesting treatment of the general theory of quasigroups, with applications to net theory. The notion of isotopy is contained therein, under the name of similarity; two quasigroups are isotopic or similar, if and only if they define isomorphic nets. The first of these papers contains moreover a number of valuable references.

It would also seem appropriate to add to the bibliography a paper on linear algebras which has just appeared [23].

REFERENCES

1. N. Jacobson, *A note on non-associative algebras*, Duke Math. J. vol. 3 (1937) pp. 544–548.

2. A. A. Albert, *Non-associative algebras*. I. *Fundamental concepts and isotopy*, Ann. of Math. (2) vol. 43 (1942) pp. 685–707; II, *New simple algebras*, loc. cit. pp. 708–723.

3. A. A. Albert, *Quasigroups*. I, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 507–519; II, Trans. Amer. Math. Soc. vol. 55 (1944) pp. 401–419.

4. R. H. Bruck, *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. vol. 55 (1944) pp. 19–52.

5. A. A. Albert, *Modern higher algebra*, Chicago, 1937.

6. L. E. Dickson, *Linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc. vol. 7 (1906) pp. 370–390.

7. Robert M. Thrall, *On projective equivalence of trilinear forms*, Ann. of Math. vol. 42 (1941) pp. 469–485.

8. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloquium Publications, vol. 24, New York, 1939.

9. W. Specht, Jber. Deutsche Math. Verein. vol. 49 (1940) pp. 207–215.

10. I.. E. Dickson, *Linear algebras*, Cambridge, England, 1914.

11. H. Hopf, *Ein topologischer Beitrag zur reellen Algebra*, Comment. Math. Helv. vol. 13 (1940–1941) pp. 219–239.

12. A. Suschkewitsch, *On a generalization of the associative law*, Trans. Amer. Math. Soc. vol. 31 (1929) pp. 204–214.

13. L. E. Dickson, *Algebras and their arithmetics*, Chicago, 1923.

14. George N. Garrison, *Quasi-groups*, Ann. of Math. vol. 41 (1940) pp. 474–487.

15. David Hilbert, *Grundlagen der Geometrie*, 7th ed., Berlin, 1930.

16. David Hilbert, *Foundations of geometry*, translated by E. J. Townsend, Chicago, 1902.

17. C. C. MacDuffee, *An introduction to abstract algebra*, New York, 1940.

18. L. E. Dickson, *Linear algebras with associativity not assumed*, Duke Math. J. vol. 1 (1935) pp. 113–125.

19. L. E. Dickson, *Linear algebras*, Trans. Amer. Math. Soc. vol. 13 (1912) pp. 59–73.

20. L. E. Dickson, *On quaternions and their generalizations and the history of the eight-square theorem*, Ann. of Math. vol. 20 (1919) pp. 155–171.

21. A. A. Albert, *Quadratic forms permitting composition*, Ann. of Math. vol. 43 (1942) pp. 161–177.

22. Reinhold Baer, *Nets and groups*, Trans. Amer. Math. Soc. vol. 46 (1939) pp. 110–141; II, loc. cit. vol. 47 (1940) pp. 435–439.

23. A. A. Albert, *Algebras derived by non-associative matrix multiplication*, Amer. J. Math. vol. 64 (1944) pp. 30–40.

University of Wisconsin,
Madison, Wis.