NEW DIVISION ALGEBRAS

BY L. E. DICKSON

1. Introduction. No technical acquaintance with linear algebras is presupposed in this note. We consider only linear algebras for which multiplication is associative. As with quaternions, an algebra \( A \) is called a division algebra if every element \( \neq 0 \) of \( A \) has an inverse in \( A \). A division algebra \( A \) over a field \( F \) is called normal if the numbers of \( F \) are the only elements of \( A \) which are commutative with every element of \( A \).

In a paper recently offered to the Transactions of this Society, A. A. Albert determined all normal division algebras of order 16 and found a new type. The object of this note is to derive from mild assumptions the corresponding type of normal division algebras \( A \) of order \( \epsilon p^2 \), where \( p \) is a prime. We shall first draw simple conclusions from an initial assumption.*

Assumption 1. Let \( A \) contain an element \( i_1 \) satisfying an equation \( f(\omega^2) = 0 \) of degree \( 2p \) with only even powers of \( \omega \), whose coefficients are in \( F \), that of \( \omega^{2p} \) being unity, and which is irreducible in \( F \), such that the polynomials in \( i_1 \) are the only elements of \( A \) which are commutative with every element of \( A \).

2. Lemma 1. Let an element \( i_2 \) of \( A \) be commutative with \( I = i_1^2 \), but not with \( i_1 \) itself. The algebra \( S \) generated by \( i_1 \) and \( i_2 \) is of order \( 4p \). It may be regarded as an algebra of order 4 with the basis 1, \( i_1 \), \( i_2 \), \( ij_1 \) over \( F(I) \); this algebra is normal. In other words, the polynomials in \( I \) are the only elements of \( S \) which are commutative with every element of \( S \).

Let \( K \) denote the field composed of all those elements of

* Except for the requirement concerning even powers of \( \omega \), Assumption 1 is proved in the writer's *Algebren und ihre Zahlentheorie*, Zürich, 1927, pp. 262–3.
which are commutative with every element of $S$. If $K$ is of order $k$ and $S$ is of order $s$ over $F$, then $S$ is a normal division algebra of order $n^2$ over $K$, where $s = n^2k$. Since $K$ contains the root $I$ of an equation of degree $p$ irreducible in $F$, the subfield $F(I)$ is of order $p$, whence $k$ is a multiple of $p$.

Since $i_2$ is not commutative with $i_1$, $i_2$ is not a polynomial in $i_1$ and hence is not a rational function of $i_1$. Thus

\[(1) \quad i_1^j, i_1^j i_2, \quad (j = 0, 1, \cdots, 2p - 1),\]

are linearly independent with respect to $F$. Hence $s \geq 4p$. Since $S$ and $A$ are normal over different fields $K$ and $F$, $S \neq A$. Thus $s$ is a divisor $<4p^2$ of $4p^2$. First, let $p > 2$.

If $s$ is not divisible by $p^2$, then $s = 4p$. But if $s$ is divisible by $p^2$, either $s = 2p^2$, or $s = p^2$ and $p > 4$. If $p = 2$, evidently $s = 8 = 4p$.

If either $s = p^2$, $p > 4$, or $s = 2p^2$, $p > 2$, then $s = n^2k$ and the divisibility of $k$ by $p$ show that $n = 1$, $S = K$, contrary to the fact that $i_2$ is not commutative with $i_1$.

Hence $s = 4p = n^2k$, whence $n = 2$, $k = p$. Thus $K = F(I)$ and $S$ is a normal algebra of order 4 over $F(I)$. The $4p$ elements (1) form a basis of $S$ over $F$.

3. **Lemma 2.** Any element of $A$ which is commutative with $I = i_1^2$ belongs to $S$.

Any element not in $S$ extends $S$ to a division subalgebra whose order exceeds $4p$, is a multiple of $4p$, and is a divisor of $4p^2$. Hence it extends $S$ to $A$ itself (of order $4p^2$).

Suppose that $e$ is commutative with $I$ and is not in $S$. Since $I$ is commutative with every element of $S$ and with $e$, which extends $S$ to $A$, $I$ is commutative with every element of $A$. Since $I$ is not in $F$, this contradicts the hypothesis that $A$ is normal over $F$.

4. **Assumption 2.** Let $A$ contain elements $i_1$ and $z$ such that $i_1$ satisfies Assumption 1 and such that

\[(2) \quad i_2 = zi_1z^{-1}, \quad i_3 = zi_2z^{-1}, \cdots, \quad i_p = zi_{p-1}z^{-1}\]
are all commutative with \( I = i_2 \), while \( i_2 \) is not commutative with \( i_1 \), and \( i_3^2 \neq I \).

Since \( z I z^{-1} = i_2^2 \neq I \), \( z \) is not commutative with \( I \) and hence is not in \( S \). By §3, \( z \) extends \( S \) to \( A \). Since (1) gives a basis of \( S \), every element of \( S \) is of the form

\[
G = p(i_1) + q(i_2)i_2.
\]

Then

\[
G' = z G z^{-1} = p(i_3) + q(i_2)i_3.
\]

For \( p \geq 3 \), \( i_3 \) is commutative with \( i_2^2 \) and hence is in \( S \). Thus

\[
zG = G'z, \ G' \text{ in } S.
\]

5. **Lemma 3.** \( i_2^2, \ldots, i_p^2 \) are all distinct.

Suppose that \( i_r^2 + i_s^2 = i_t^2 \), where \( r \) is one of \( 2, 3, \ldots, p-1 \). Then

\[
z^r i_r^2 z^{-r} = i_{r+1}^2 = i_t^2,
\]

whence \( z^r \) is commutative with \( i_t^2 \) and is in \( S \). Using also (5), we see that every element of the algebra \( A \) obtained by extending \( S \) by \( z \) is of the form

\[
H_0 + H_1 z + \cdots + H_{r-1} z^{r-1},
\]

where each \( H \) is in \( S \). Since \( S \) is of order \( 4p \), the order of \( A \) is \( \leq 4p \cdot r < 4p^2 \). But \( A \) is of order \( 4p^2 \).

Suppose that \( i_{r+s+1}^2 = i_r^2 \) \((r>0, s>1)\). These are the transforms of \( i_{r+s+1}^2 \) and \( i_{r-1}^2 \) by \( z \). Hence the latter are equal. After \( s-1 \) such steps, we get \( i_{r+s+1}^2 = i_r^2 \), just proved impossible.

6. **Lemma 4.** We have the following identity:

\[
f(e) = (e - i_p^2) \cdots (e - i_2^2)(e - i_1^2).
\]

Note that

\[
i_r \text{ is commutative with } i_{r+1}, \ldots, i_p, \ (r=1, \ldots, p-1).
\]

This is true by Assumption 2 if \( r = 1 \). To proceed by induction, let (7) hold when \( r = j \), whence \( i_j^2 \) is commutative.
with $i_k$ for $k \geq j + 1$. Transformation by $z$ shows that $i_{j+1}^2$ is commutative with $i_{k+1}$, whence (7) holds when $r = j + 1$.

Write $v_j$ for $i_j^2$. As a special case of (7), $v_1, \ldots, v_p$ are commutative. The indeterminate $\epsilon$ is commutative with every quantity of $A$. Thus $z$ transforms $f(\epsilon)$ into itself. But $f(v_1) = 0$. Hence by (2), $f(v_2) = 0, \ldots, f(v_p) = 0$. Let

$$f(\epsilon) = \sum_{j=0}^p a_j \epsilon^{p-j}, \quad q(\epsilon) = \sum_{j=0}^{p-1} c_j \epsilon^{p-1-j}, \quad a_0 = c_0 = 1,$$

$$c_j = a_j + c_{j-1}v_1, \quad (j = 1, \ldots, p).$$

Then, since $v_1$ is commutative with $\epsilon$,

$$f(\epsilon) \equiv q(\epsilon)(\epsilon - v_1) + c_p.$$  \hspace{1cm} (8)

By induction on $r$,

$$c_r = \sum_{j=0}^r a_j v_1^{r-j}, \quad c_p = f(v_1) = 0.$$  \hspace{1cm} Since $v_1$ is commutative with $v_1$, we obtain a true equality from (8) by replacing $\epsilon$ by $v_1$. Thus $0 = q(v_i)(v_i - v_1)$. The second factor is not zero if $i \geq 2$. In our division algebra we therefore have $q(v_i) = 0$ when $i \geq 2$.

We may repeat this argument with $f$ and $v_1$ replaced by $q$ and $v_2$. Hence $q(\epsilon) = r(\epsilon)(\epsilon - v_2)$, in which the coefficients of $r(\epsilon)$ are polynomials in $v_1$ and $v_2$. Since they are commutative with $v_i$, $0 = r(v_i)(v_i - v_2)$. Hence $r(v_i) = 0$ when $j \geq 3$.

Proceeding similarly, we ultimately obtain

$$f(\epsilon) \equiv (\epsilon - v_p) \cdots (\epsilon - v_2)(\epsilon - v_1).$$

7. **Theorem 1.** $f(\epsilon) = 0$ is a cyclic equation.

By (6), $i_1^2 + \cdots + i_p^2$ is a number of $F$ and hence is transformed into itself by $z$. But $z$ transforms $i_1^2$ into $i_2^2$, $i_2^2$ into $i_3^2$, $\cdots$, $i_{p-1}^2$ into $i_p^2$. Hence $z$ must transform $i_p^2$ into $i_1^2$. Since $z^p$ transforms $i_1^2$ into $i_2^2$, $z^{p-1}$ transforms $i_2^2$ into $i_3^2$ and evidently transforms $i_1$ into $i_p$. Hence $z^p$ transforms
$i^2_1$ and $i_1i^2_2$ into $i^2_1i_p$ and $i_p^2i^2_2$. The latter are equal by
by Assumption 2. Hence the former are equal. Since $i^2_2$ is
therefore commutative with both generators $i_1$ and $i_2$ of $S$, it is
commutative with every element of $S$. By Lemma 1,
$i^2_2 = \theta(i^2_2)$, where $\theta$ is a polynomial with coefficients in $F$.
Transformation by $z$ gives
\[
\theta(i^2_2) = \theta[i^2_2] = \theta^p(i^2_2),
\]
if $\theta^r(k)$ denotes the $r$th iterative of $\theta(k)$ and not its $r$th
power. By induction,
\begin{align}
\theta(i^2_2) & = \theta^r(i^2_2). 
\tag{9}
\end{align}
Take $r = p - 1$ and transform by $z$. Hence
\begin{align}
\theta(i^2_2) & = \theta^{p-1}(i^2_2) = \theta^p(i^2_2). 
\tag{10}
\end{align}
Since $f(\epsilon) = 0$ has these properties, it is cyclic.

8. Theorem 2. Every element of $A$ can be expressed in one
and only one way in the form
\begin{align}
A_0 + A_1z + \cdots + A_{p-1}z^{p-1}, 
\tag{11}
\end{align}
where each $A_i$ is in $S$. The product any two sums (11) can be
expressed as a third such sum by means of
\begin{align}
zG & = G'z, \quad z^p = s, 
\tag{12}
\end{align}
where $G, G', s$ are all in $S$ and are defined in (4), (5).

Since $z^{p-1}$ transforms $i^2_2$ into $i^2_2$, and $z$ transforms the
latter into the former, $z^p$ is commutative with $i^2_2$ and hence
is in $S$. By means of (12), every element of $A$ (to which
$z$ extends $S$) can be expressed in the form (11). Since $S$
and $A$ are of orders $4p$ and $4p^2$, two polynomials (11) are
distinct unless identical.

9. Theorem 3. $S$ is an algebra of generalized quaternions
over $F(I)$ with the basis $1, i_1, y, i_1 y$, where $y = i_1i_2 - i_2i_1$.

Since $i_2$ is not commutative with $i_1$, $y \neq 0$. Since $i_2$ is
commutative with $i^2_2$,
(13) \[ yi_1 = -i_1 y. \]

Thus \( y \) is not commutative with \( i_1 \) and hence is not a polynomial in \( i_1 \). We may therefore replace the basis (1) of \( S \) over \( F \) by \( i_1^i, i_1^i y \). Thus \( S \) has the basis in Theorem 3.

By §7, \( i_2^2 \) is commutative with \( i_1 \). Hence
\[
r = i_1 i_2 + i_2 i_1
\]
is commutative with \( i_2 \). Since \( i_2 \) is commutative with \( I = i_2^2, r_i = i_2 r \). Hence \( r \) is commutative with every element of \( S \). Thus \( r \) is a polynomial \( P(I) \) in \( I \). We have
\[
2i_1 i_2 = P(I) + y, 2i_2 i_1 = P(I) - y.
\]

But \( y \) is commutative with \( I \). Hence
\[
4i_1 i_2 i_1 = P^2 - y^2.
\]

Since \( i_2^2 \) is commutative with \( i_1 \),
\[
y^2 = [P(I)]^2 - 4I \theta(I).
\]

This fact that \( y^2 \) is a polynomial in \( I \) and relation (13) together show that \( S \) is an algebra of generalized quaternions over \( F(I) \).

The University of Chicago