A NOTE ON NORMAL DIVISION ALGEBRAS OF ORDER SIXTEEN*

BY A. A. ALBERT

1. *Introduction.* I have proved† that every normal division algebra of order sixteen over any non-modular field F contains a quartic field with G_4 group. This important result gave a *determination of all normal division algebras of order sixteen.* I have recently proved‡ the existence of *non-cyclic* normal division algebras, so that the result mentioned above is actually the best possible result. However, my proof of 1929 is long and complicated and the above result there obtained is of sufficient importance to make a better proof desirable. It is the purpose of this note to provide such a proof.

2. *Results Presupposed.*§ We shall require certain well known results on normal division algebras D of order sixteen over F. Algebra D has rank four, so that every sub-field of D is either a quartic field, a quadratic field, or F itself. We also have the following theorems.

THEOREM 1. *Every root in D of the minimum equation of a quantity x of D is a transform yxy^{-1} of x by y in D.*

THEOREM 2. *If $\phi(\omega)=0$ is the minimum equation of x in D, then there exist quantities $x_i=x_1, x_2, \cdots, x_r$ in D such that*

$$\phi(\omega) \equiv (\omega - x_r) \cdots (\omega - x_2)(\omega - x_1).$$

It is obvious that no two adjacent transforms x_{i+1}, x_i in the above irreducible equation can be equal.

From the well known Wedderburn theorem on linear associative algebras with normal simple sub-algebras we have immediately the following result.

* Presented to the Society, August 31, 1932.

† Transactions of this Society, vol. 31 (1929), pp. 253–260.

‡ See this Bulletin of June 1932 and the Transactions of this Society of January 1933 for proof.

§ See my paper, Annals of Mathematics, vol. 30 (1929), pp. 322–338, for a proof of Theorem 1 and a reference to proofs of Theorem 2 and the Wedderburn result implying Theorem 3.

THEOREM 3. *Let D contain a generalized quaternion algebra Q. Then $D=Q\times R$, where R is also a generalized quaternion algebra.*

3. *On Quartic Fields.* Let X be a quartic field over F. If $X=F(x)$, so that x generates X, then x is called a *primitive* quantity of X, otherwise *imprimitive*. Similarly X is *primitive* if it contains no imprimitive quantities not in F and otherwise is *imprimitive*. The *group* of X is *primitive* or *imprimitive* according as X is primitive or imprimitive.* In a quartic field X the only possible sub-fields except F are those of order two. Hence X is imprimitive if and only if it has a quadratic sub-field.

If x is any primitive quantity of X and the minimum equation of x is $\phi(\omega)=0$, then X is known† to be imprimitive if X contains an $x_2 \neq x$ and yet satisfying $\phi(\omega)=0$.

Of particular importance for us are quartic fields X with group

$$(1)\qquad G_4=(I,\, s_1,\, s_2,\, s_3),\; s_1^2=s_2^2=s_3^2=I,\; s_3=s_1s_2=s_2s_1.$$

Obviously the above group is the direct product of two cyclic groups of order two. Correspondingly, X is the direct product of two quadratic fields. Conversely, every direct product of two non-equivalent quadratic fields is a quartic field with group G_4. We shall prove that every normal division algebra D of order sixteen over D contains two quadratic sub-fields $F(u)$, $F(v)$ such that $uv=vu$, while v is not in $F(u)$. It follows that the sub-field $F(u,\, v)$ of the division algebra D is the direct product of $F(u)$ and $F(v)$ and has group G_4.

4. *The Existence of a Quadratic Sub-Field of D.* We shall first prove the following lemma.

LEMMA. *Let x in D have*

$$(2)\qquad \phi(\omega)\equiv\omega^4+\alpha\omega^3+\beta\omega^2+\gamma\omega+\delta=0,\qquad (\alpha,\cdots,\delta \textit{ in } F),$$

as its minimum equation and let Y be a quartic field such that

$$(3)\qquad \phi(\omega)\equiv B\cdot A$$

where

$$(4)\qquad A\equiv\omega^2-t_1\omega+s_1,\quad B\equiv\omega^2-t_2\omega+s_2$$

* See Weber's *Algebra*, vol. 1, p. 505 and p. 525 for the preceding results.

† See Netto's *The Theory of Substitutions*, p. 198.

have coefficients t_1, t_2, s_1, s_2 *in* Y. *Then one of* $X=F(x)$ *and* Y *is imprimitive.*

For let W be an extension of Y in which A and B are reducible. Then $A\equiv(\omega-\xi_2)(\omega-\xi_1)$, $B\equiv(\omega-\xi_4)(\omega-\xi_3)$, where $\xi_1, \cdots, \xi_4$ are in W so that the fields $X=F(x)$, $F(\xi_i)$ are equivalent quartic fields. If $s_1=\lambda$ in F, then $\xi_2\xi_1=\lambda$, $\xi_2=\lambda\xi_1^{-1}\neq\xi_1$ is in $F(\xi_1)$. Hence $F(\xi_1)$ and $F(x)$ are imprimitive by the argument of §3.

If $s_2+s_1=\lambda$ in F, then, since $s_2s_1=\delta$ in F, s_1 is a root of $\omega^2-\lambda\omega+\delta=0$ and, since s_1 is not in F, Y containing s_1 is imprimitive. Hence let $y=s_1+s_2$ be not in F.

But $y=\xi_4\xi_3+\xi_2\xi_1$ is well known,* by elementary theory of quartic equations, to be a root of the resolvent cubic of $\phi(\omega)=0$. Hence $F(y)$ cannot have order four. Hence Y is imprimitive. Our proof of the lemma is complete.

Let now x be in D and $X=F(x)$ be a *primitive* quartic field. By Theorem 2

$$\phi(\omega)\equiv(\omega-x_4)(\omega-x_3)(\omega-x_2)(\omega-x_1),\ x_1=x, \tag{5}$$

where x_2, x_3, x_4 are in D. Also

$$\begin{aligned}\phi(\omega)&\equiv B\cdot A,\quad B\equiv(\omega-x_4)(\omega-x_3)\equiv\omega^2-t_2\omega+s_2,\\ A&\equiv(\omega-x_2)(\omega-x_1)\equiv\omega^2-t_1\omega+s_1.\end{aligned} \tag{6}$$

Using (6) and (2) and comparing coefficients of ω^3, ω^2, $\omega^0=1$, respectively, we obtain

$$t_2+t_1=-\alpha,\ s_2+s_1+t_2t_1=\beta,\ s_2s_1=\delta. \tag{7}$$

By substituting for s_2 and t_2 from the first and third parts of (7) in its second part we obtain

$$\delta s_1^{-1}+s_1=\beta+t_1\alpha+t_1^2\,. \tag{8}$$

Suppose that both $F(s_1)$ and $F(t_1)$ are *primitive*. Then any quantity of each field generates the field and the two fields are equal if and only if they have a quantity not in F in common. But $t_1^2+\alpha t_1+\beta$ is not in F and is in $F(s_1)$ by (8). Hence $F(t_1)=F(s_1)=Y$ contains all of s_1, s_2, t_1, t_2 by (7). But X is a primitive field by hypothesis. Hence, by the above lemma, Y is imprimitive, a contradiction.

* See L. E. Dickson, *First Course in the Theory of Equations*, p. 51. Thus the above essential point of our proof is a very elementary result.

Hence at least one of $F(s_1)$, $F(t_1)$ is imprimitive and contains a quadratic sub-field, or one of these fields is a quadratic field, or one of them coincides with F. But if either $t_1=x_2+x_1$ or $s_1=x_2x_1$ is in F, then X contains a root $x_2\neq x_1$ of the minimum equation of x_1 and is imprimitive, a contradiction.

Hence if x is in D but not in F, then either $F(x)$ is a quadratic field, or $F(x)$ is imprimitive and contains a quadratic field, or $F(x)$ is primitive but either $F(s_1)$ or $F(t_1)$ contains a quadratic field. We have thus proved the following theorem.

THEOREM 4. *Every normal division algebra of order sixteen over F contains a quadratic sub-field.*

The above proof is certainly a great simplification of my earlier proof of the same theorem requiring about four printed pages. We shall also obtain a simpler proof of the final result, a consequence of Theorem 4.

5. *The Desired Determination.* Let D be a normal division algebra of order sixteen over F. By Theorem 4, D contains a quadratic sub-field $U=F(u)$, $u^2=\rho$ in F. But $(-u)^2=\rho$ so that, by Theorem 1, $-u=yuy^{-1}$, where y is in D. From $yu=-uy$ it follows that $y^2u=uy^2$. If $y^2=\lambda$ in F, algebra D contains the generalized quaternion algebra $Q=(1, u, y, uy)$ over F and, by Theorem 3, $D=Q\times R$, where $R=(1, v, z, vz)$, $zv=-vz$, $v^2=\sigma$ in F. In this case D contains the quartic field $F(u, v)$ with G_4 group as desired. Let then $y^2=v$ not in F. If v is a primitive quantity of $Y=F(y)$, then Y is a polynomial in y^2. But y^2 is commutative with u while y is not commutative with u. Hence v is imprimitive, $vu=uv$, $F(v)$ is a quadratic field. Also u is obviously not in $F(v)<F(y)$ so that $F(u, v)$ is a quartic field with group G_4. The following theorem is thus proved.

THEOREM 5. *Every normal division algebra of order sixteen over any non-modular field F contains a quartic sub-field with group G_4.*

THE UNIVERSITY OF CHICAGO