ON NORMAL DIVISION ALGEBRAS OF TYPE R IN THIRTY-SIX UNITS*

BY
A. ADRIAN ALBERT

1. Introduction. A normal division algebra in \( n^2 \) units over a non-modular field \( F \) is of type \( R \) if it contains a quantity \( i \) whose minimum equation with respect to \( F \), \( \phi(\omega) = 0 \), has degree \( n \) and \( n \) distinct roots which are polynomials in \( i \) with coefficients in \( F \). Algebras of type \( R \) occupy a central position in the theory of division algebras as they are the only normal division algebras whose structure is known, and all division algebras of order less than twenty-five are expressible as algebras of type \( R \).

The normal division algebras \( D \) whose structure is the simplest are those for the case where \( \phi(\omega) = 0 \) has the cyclic group with respect to \( F \). When \( n \) is six and \( \phi(\omega) = 0 \) is cyclic, \( D \) is expressible as the direct product of a generalized quaternion division algebra and a cyclic division algebra of order nine, while conversely every such direct product is a cyclic division algebra of order thirty-six. The group of \( \phi(\omega) = 0 \) is evidently regular and hence the only other type of equation to be considered for algebras of order thirty-six and type \( R \) is one which has the single non-cyclic, non-abelian regular group on six letters, a case giving a very complicated algebra.

It has never been demonstrated that there exist normal division algebras which are not cyclic algebras. The author showed, in a recent paper,† that the algebras which had been constructed by F. Cecioni‡ and which were based on a non-cyclic quartic were cyclic algebras. We show here that all normal division algebras of type \( R \) in thirty-six units are cyclic algebras.

2. Algebras based on a non-cyclic sextic with regular group. Let \( D \) be an associative normal division algebra of order thirty-six and type \( R \), and let \( i \) be the quantity of \( D \) which defines the type of \( D \). If \( \phi(\omega) = 0 \), the minimum equation of \( i \), is a cyclic sextic, \( D \) is called a cyclic algebra. There remains to be considered the case where the group of \( \phi(\omega) = 0 \) is non-cyclic. The author has shown|| that \( \phi(\omega) \) may be taken to have only even powers of the indeterminate \( \omega \) and that there exists a polynomial \( \theta(i) \) in \( F(i) \) such that

---

* Presented to the Society, October 25, 1930; received by the editors in August, 1930.
† These Transactions, vol. 32 (1930), pp. 171–195.
while for the non-cyclic case

\[\theta^2(i) = i, \quad \theta(-i) = -\theta^2(i), \quad \theta^2(-i) = -\theta(i).\]

Evidently \(i^2\) satisfies a cubic equation irreducible in \(F\), and \(F(i^2)\) is a cubic field over \(F\). The set of all quantities in \(F(i)\) which are symmetric in \(i, \theta(i), \theta^2(i)\), form a quadratic sub-field

\[K = F(v), \quad v^2 = \rho \text{ in } F,\]

of \(F(i)\). A cubic field contains no quadratic sub-field so \(v\) is not in \(F(i^2)\). Hence \(1, v\) are linearly independent with respect to \(F(i^2)\), and every quantity in \(F(i)\) is expressible in the form

\[a = a(i) = a_1 + a_2v \quad (a_1 \text{ and } a_2 \text{ in } F(i^2)).\]

But then

\[i = p_1 + pv\]

with \(p\) and \(p_1\) in \(F(i^2)\), so that

\[i^2 = (p_1^2 + p^2\rho) + 2p_1pv, \quad 0 = (p_1^2 + p^2\rho - i^2) + 2p_1pv.\]

It follows that \(2p_1p = 0\). If \(p\) were zero then \(i\) would be in \(F(i^2)\), a cubic field, contrary to the fact that \(F(i)\) is a field of order six. Hence \(p_1\) is zero and

\[i = pv, \quad p \text{ in } F(i^2).\]

It is known* that \(D\) has a basis

\[i^sj, \quad i^sj^t \quad (s = 0, 1, \ldots, 5; t = 0, 1, 2),\]

and a multiplication table

\[\phi(i) = 0, \quad j^ta = a[\theta^t(i)]j^t \quad (t = 0, 1, \ldots),\]

\[za(i) = a(-i)z, \quad zj = \alpha j^2z, \quad zj^2 = \alpha [\theta^2(i)]gjz,\]

\[j^3 = g, \quad z^2 = \gamma,\]

for every \(a\) in \(F(i)\) where \(g, \alpha, \gamma\) are in \(F(i)\). Since \(zz^2 = z^2z\) we have \(\gamma = \gamma(-i)\) is in \(F(i^2)\). Similarly \(jg = gj\) gives \(g = g[\theta(i)]\) is in \(F(v)\). Write

\[\gamma = \gamma_1 + \gamma_2i^2 + \gamma_3i^4 \quad (\gamma_1, \gamma_2, \gamma_3 \text{ in } F),\]

and suppose that \(\gamma_3 \neq 0\). We can then define scalars \(\gamma_4, \gamma_5\) in \(F\) by \(\gamma_1 = \gamma_3\gamma_5, \gamma_2 = 2\gamma_3\gamma_5\) and

* See L. E. Dickson, Algebren und ihre Zahlentheorie, pp. 75–79, where \(q = 2, z = j_0, j = j_1, \theta_0(i) = -i, \theta_1(i) = \theta(i).\)
\[ \gamma = \gamma_1(i^4 + 2\gamma_2 i^2 + \gamma_6 - \gamma_8^2) = \gamma_3(i^2 + \gamma_6)^2 + \gamma_3(\gamma_6 - \gamma_8^2). \]

Consider the quantity
\[ i_1 = (i^2 + \gamma_6)v. \]

Since \( v \neq 0 \) we have \( v^2 = \rho \neq 0 \) in a division algebra and
\[ i_1^2 = (i^2 + \gamma_6)^2 \rho = \rho i^4 + 2 \rho i^2 \gamma_6 + \rho \gamma_8^2 \]
is in \( F(i^2) \) but not in \( F \), since in particular the coefficient of \( i^4 \) is not zero. But \( F(i^2) \) has no proper sub-field other than \( F \), so that \( F(i^2) = F(i^2) \). The quantities
\[
(i^2 + \gamma_6)v, \quad -(i^2 + \gamma_6)v, \quad [\theta(i)^2 + \gamma_6]v, \\
- [\theta^2(i)^2 + \gamma_6]v, \quad [\theta^2(i)^2 + \gamma_6]v, \quad [\theta(i)^2 + \gamma_6]v
\]
are transforms
\[ i_1, \quad z_i z_i^{-1}, \quad j_i j_i^{-1}, \quad z_i j_i (z_i j_i)^{-1}, \quad j_i^2 i_i j_i^{-2}, \quad z_i^2 i_i (z_i^2 j_i)^{-2} \]
of \( i_1 \) and are roots of its minimum equation. If they were not distinct, two of
\[ \pm (i^2 + \gamma_6), \quad \pm [\theta(i)^2 + \gamma_6], \quad \pm [\theta^2(i)^2 + \gamma_6] \]
would be equal, which is impossible since those with plus signs are the distinct roots of the irreducible cubic minimum equation of \( i^2 + \gamma_6 \), while this cubic has not the negative of any one of its roots as a root since it has not even powers only. The minimum equation of \( i_1 \) has thus six distinct roots in \( F(i) \) so that its degree is six, \( F(i_1) \) contained in \( F(i) \) has order six, and \( F(i_1) = F(i) \). Evidently \( z_i = -i z_i \), while \( j \) transforms \( i \) into a quantity in \( F(i_1) \), that is a polynomial in \( i_1 \). We may thus replace \( i \) by \( i_1 \) in the basis of \( D \) without loss of generality, and, since \( \gamma = (\gamma_8 \rho^{-1}) i^2 + \gamma_3 (\gamma_6 + \gamma_8^2) \), for this new \( i \) we have \( \gamma \) expressed as a linear combination with coefficients in \( F \) of 1 and \( i^2 \). When \( \gamma_3 = 0 \) we also have immediately such an expression, so that we have proved

**Lemma 1.** The quantity \( i \) may be so chosen that, without altering any other property of \( D \),
\[
\gamma = \gamma_1 + \gamma_3 i^2 \quad (\gamma_1 \text{ and } \gamma_2 \text{ in } F).
\]

We shall utilize the notations
\[
(a')' = a(- i), \quad a_\theta = a[\theta(i)], \quad a_{\theta \theta} = (a_\theta)_\theta, \quad (a')_\theta = (a_{\theta \theta})', \quad (a')_{\theta \theta} = (a_\theta)',
\]
so that from (2) we immediately have
\[
(a')' = a, \quad (a_\theta)_{\theta \theta} = (a_{\theta \theta})_\theta = a, \\
(a')_{\theta \theta} = (a_{\theta \theta})', \quad (a')_\theta = (a_{\theta \theta})'.
\]
for every $a$ of $F(i)$. Also

\[ ja = a_0j, \quad j^2a = a_0j^2, \quad za = a'z, \]

from (7), while

\[ i' = -i, \quad v' = -v, \quad v_0 = v, \quad (i^2)' = i^2, \quad g = g_0 = g_0, \quad \gamma = \gamma'. \]

Consider the quantities

\[ d = \lambda_1 + \lambda_4i, \quad e = \lambda_2 + \lambda_3i, \]

where

\[ 2\lambda_1 = 1 + \gamma_1, \quad 2\lambda_2 = 1 - \gamma_1, \quad 2\lambda_3 = 1 + \gamma_2, \quad 2\lambda_4 = 1 - \gamma_2, \]

so that $\lambda_1, \ldots, \lambda_4$ are in $F$, $\lambda_1^2 - \lambda_2^2 = \gamma_1$, $\lambda_3^2 - \lambda_4^2 = \gamma_2$. Then

\[ dd' - ee' = \lambda_1^2 - \lambda_2^2 - (\lambda_3^2 - \lambda_4^2 i^2) = \gamma_1 + \gamma_2 i^2 = \gamma. \]

But $\gamma = \gamma'$ and if we put $f = d\gamma^{-1}$, $h = e\gamma^{-1}$, we have

\[ (ff' - hh')\gamma = (dd' - ee')\gamma^{-1} = 1, \]

and obtain

**Lemma 2.** There exist polynomials $f$ and $h$ in $F(i)$ such that

\[ (ff' - hh')\gamma = 1. \]

Let now $r$ and $s$ be defined by

\[ r = \alpha f, \quad s = \alpha h, \]

where $\alpha$ is the quantity of (7) such that $zj = \alpha j^2z$ and $\alpha$ is in $F(i)$. Then $r$ and $s$ are in $F(i)$, and

\[ (rr' - ss')\gamma(\alpha^{-1})(\alpha^{-1})' = 1. \]

But if $\delta = (jz)^2 = jsz = j\alpha j^2sz = \alpha \epsilon \gamma$, then $\delta_0 = j(jz)j^{-1} = (j\alpha j^2)^2 = (\alpha^{-1}\alpha j^2)^2 = (\alpha^{-1}j)^2 = (\alpha^{-1})^2 \gamma$, so that (18) gives

**Lemma 3.** There exist quantities $r$ and $s$ in $F(i)$ such that, if

\[ \delta = (jz)^2 = \alpha \epsilon \gamma, \]

then

\[ (rr' - ss')\delta_0 = 1. \]

If $a$ and $b$ are defined by

\[ a = sa^{-1}, \quad b = r\theta, \]

so that $b_\theta = r$, then

\[ Q = [b_\theta(b_\theta)'^{-1} - aaa'^{-1}], \quad Q\delta_0 = 1. \]
3. The cyclic property. We shall now proceed to prove that \( D \) is a cyclic algebra by the use of our fundamental existence theorem, Lemma 3. Consider the quantity

\[
X = a + bj + cj^2,
\]

where we take \( a \) and \( b \) to be the polynomials of Lemma 3 which satisfy (22) and where \( c \) will be chosen to be a polynomial in \( i \) with coefficients in \( F \). For every \( c \) in \( F(i) \), we have

\[
zXz^{-1} = X' = a' + c\alpha_{11}gj + b'\alpha j^2,
\]

so that

\[
XX' = (a + bj + cj^2)(a' + c\alpha_{11}gj + b'\alpha j^2) = A + Bj + Ej^2,
\]

where \( A \) is a polynomial in \( i \) and

\[
B = ac\alpha_{11}g + b(a')g + c(b'\alpha)g = Rc + Sc' + T,
\]

\[
E = ab'\alpha + b(c'\alpha_{11}g3) + c(a')g = Gc + H(c')g + K.
\]

The quantities \( B \) and \( E \) are polynomials in \( i \) and we have defined above

\[
R = (b'\alpha)g3 = (b_{111}g3), \quad S = a\alpha_{11}g, \quad T = b(a')g = b(a_{11})',
\]

\[
G = (a')g = (a'g)', \quad H = b\alpha_{11}g, \quad K = ab'\alpha,
\]

all in \( F(i) \). Now

\[
(g')g = (g_{11})' = g', \quad (g')g3 = [(g')g]g = (g')g = g.
\]

Transforming \( B \) by \( z \) we have

\[
B' = R'c' + S'c + T',
\]

whence

\[
R'B - SB' = R'Rc + R'Sc' + R'T - SR'c' - SS'c - ST' = (RR' - SS')c - (ST' - R'T).
\]

But

\[
RR' - SS' = (b_{111}g3)(a_{111}g3)'g' - a\alpha_{11}g3a'\alpha'(a_{111})'g' = gg'\alpha_{11}g3[b_{111}(b_{111})' - a\alpha a'] = gg'\alpha_{11}g3(\alpha_{111})'Q.
\]

From (19) \( \delta = \alpha_{111}g3\gamma, \) so that, utilizing the relation \( Q\delta = 1, \) we have

\[
RR' - SS' = gg'\alpha_{11}g3(\alpha_{111})'\delta^{-1} = g'(\alpha_{111})'(\gamma )^{-1} \neq 0,
\]

since \( g, \alpha \) and \( \gamma \) are all not zero in a division algebra. Hence \( RR' - SS' \) has an inverse \( (RR' - SS')^{-1} \) in \( F(i) \), and if we define the quantity \( c \) by
(35) \[ c = (ST' - R'T)(RR' - SS')^{-1}, \]
then
(36) \[ R'B - SB' = (ST' - R'T) - (ST' - R'T) = 0. \]

We shall henceforth consider the quantity \( X \) as completely defined in (23) with the \( a \) and \( b \) of Lemma 3 and the \( c \) of (35), so that (36) is satisfied. Transforming (36) by \( z \) we have
(37) \[ RB' - BS' = 0, \]
whence
(38) \[ R(R'B - SB') + S(- BS' + RB') = B(RR' - SS') = 0. \]

But \( RR' - SS' \) has an inverse in \( F(i) \), whence \( B = 0. \)

We consider now the polynomial \( E \). We first compute
(39) \[ ST' - R'T = a\alpha a\alpha b'a\alpha - b\alpha(a\alpha)'g'b(a\alpha)' \]

Next
(40) \[ H(K')_e - (G')_eK = b\alpha c\alpha g(a\alpha)'b\alpha(a\alpha)' - a\alpha b\alpha b'g' \]

so that
(41) \[ - a\alpha g[b\alpha c\alpha g(a\alpha)'(G')_e - H(H')_e] = b\alpha g[(a\alpha)'(a\alpha)'(g')^2]. \]

But \( j^2 = g, g' = zg^{-1} = zg^{-1} = (zg^{-1})^3 = (a\alpha j^2z^{-1})^3 = (a\alpha j^2z^2z^{-1})^3 = (a\alpha j^2z^2z^2) = a\alpha g(a\alpha g^2), \)
and we have the relations
(42) \[ g' = a\alpha a\alpha g^2, \]
(43) \[ g = a'(a\alpha)'(g')^2 = a'(a\alpha)'(a\alpha)'(g')^2. \]

Substituting (42) in (41) and comparing with (39) we write immediately
(44) \[ ST' - R'T = a\alpha g[H(K')_e - (G')_eK]. \]

We also have, by the use of (11), \([a\alpha]'_g = [(a\alpha)_e]_g = a\alpha', \)
(45) \[ G(G')_e - H(H')_e = (a\alpha)'a\alpha - b\alpha c\alpha g(b')_e(a\alpha)'a\alpha g'. \]

But then
(46) \[ g(a\alpha')_e [G(G')_e - H(H')_e]. \]
\[ = (a\alpha c\alpha g^2) [a'(a\alpha)'(a\alpha)_{e}g']b(b')_e - g(a\alpha(a\alpha)'g(a\alpha)'_{e}g_{e}. \]

which by (42) and (43) has the value
(47) \[ g[b(b')_e - a\alpha a\alpha (a\alpha)_{e}g(a\alpha)'_{e}]. \]
But if

\[(48) \quad Q = b_0(b_0)' - \alpha \alpha' \alpha' = b_0(b_0)' - \alpha \alpha' \alpha',\]

then from (22), \(\delta_Q = 1, Q \neq 0,\)

\[(49) \quad Q_{oo} = b(b)'_0 - \alpha \alpha' \alpha'\alpha'(\alpha')_0\alpha'\alpha'(\alpha')_0\alpha'\]

Hence

\[(50) \quad - \alpha \alpha' \alpha'(\alpha')_0 \alpha' \alpha'(\alpha')_0 \alpha' \alpha'(\alpha')_0 [G(G')_0 - H(H')_0] = gQ_{oo} \neq 0,\]

so that

\[(51) \quad \frac{H(K')_0 - (G')_0 K}{G(G')_0 - H(H')_0} = \alpha \alpha' \alpha'(\alpha')_0 \alpha' \alpha'(\alpha')_0 \alpha' \alpha'(\alpha')_0 [G(G')_0 - H(H')_0] = \frac{(\alpha')_0 [ST' - R'T]}{gQ_{oo}}.\]

From (22) we have \(\delta_Q = 1,\) so that

\[(52) \quad j^2(\delta_Q)j^{-2} = 1 = \delta Q_{oo} = \delta g Q,\]

whence

\[(53) \quad \frac{\delta Q}{\gamma} = \frac{\delta g Q}{\gamma}.\]

Now \(\delta = \gamma \alpha g\) from (19), while \(\delta = (jz)^2\) is commutative with \(jz\) and equals its transform by \(jz\), the quantity \((\delta')_g\). Hence

\[(54) \quad g = g_0, \quad \alpha g = \frac{\delta}{\gamma}, \quad \alpha \alpha g = \frac{\delta_0}{\gamma_0}, \quad \alpha g = \frac{\delta_0}{\gamma_0},\]

and

\[(55) \quad (\alpha')_g' = \frac{(\delta_0)_g'}{(\gamma_0)_g'} = \frac{(\gamma')_g}{(\gamma')_g} = \frac{\delta}{\gamma},\]

since \(\gamma = \gamma'.\) Equation (53) becomes

\[(56) \quad \alpha \alpha g Q = \alpha g' Q_{oo}.\]

From (43) \(g = \alpha'(\alpha')_0 (\alpha')_0 (g')^2,\) so that

\[\alpha' g' Q_{oo} = (\alpha' g') [(\alpha')_0 (\alpha')_0 g'] \alpha \alpha g Q,\]

and

\[(57) \quad Q_{oo} = (\alpha')_0 (\alpha' g') \alpha \alpha g Q.\]

It follows now that

\[(58) \quad g Q_{oo} (\alpha')_0 = gg' \alpha' g' (\alpha' g') Q = RR' - SS',\]
by (33). Using (35) and (51) we have

\[
(59) \quad c = (ST' - R'T)(RR' - SS')^{-1} = [H(K')_\theta - (G')_\theta K][G(G')_\theta - H(H')_\theta]^{-1}.
\]

We have now demonstrated that

\[
(60) \quad [G(G')_\theta - H(H')_\theta]c - [H(K')_\theta - (G')_\theta K] = 0,
\]
a relation very similar to (36). In fact, since \(E\) is given by (27), and \([[c']_\theta]^t = c_{\theta,\theta}, (c_{\theta,\theta})_\theta = c\),

\[
(61) \quad (E')_\theta = (G')_\theta (c')_\theta + (H')_\theta c + (K')_\theta,
\]
so that, by (60),

\[
(62) \quad (G')_\theta E - H(E')_\theta = (G')_\theta Gc + (G')_\theta H(c')_\theta + (G')_\theta K
\]

\[- H(G')_\theta (c')_\theta - H(H')_\theta c - H(K')_\theta
\]

\[= [G(G')_\theta - H(H')_\theta]c - [H(K')_\theta - (G')_\theta K] = 0.
\]

Transforming (62) by \(jz\) we have

\[
(63) \quad G(E')_\theta - (H')_\theta E = 0,
\]
and

\[
(64) \quad 0 = G[(G')_\theta E - H(E')_\theta] + H[G(E')_\theta - (H')_\theta E] = [G(G')_\theta - H(H')_\theta]E = 0.
\]

It follows from (50) that \(E = 0\) and that (25) becomes

\[
(65) \quad XX' = A \text{ in } F(i).
\]

But then

\[
(66) \quad (Xz)^2 = XzXz = XX'\gamma = A\gamma = t \text{ in } F(i),
\]

since \(\gamma\) is in \(F(i)\), and \(X'\) was defined so that \(zX = X'z\) in (24).

Let first \(b\) and \(a\) be both not zero, so that since \(Xz\) is commutative with its square,

\[
tXz = (ta + tbj + tcj^2)z = Xzt = (a + bj + cj^2)t'z.
\]

Hence

\[
ta + tbj + tcj^2 = t'a + (t')_\theta bj + (t')_\theta cj^2,
\]

and since (6) are a basis of \(D\), \(ta = t'a, tb = (t')_\theta b\). Since \(a\) is not zero, \(t = t'\) is in \(F(i^2)\). Since also \(b\) is not zero, \(t = (t')_\theta = t_\theta\) is in \(F\). It follows that when \(ab \neq 0\) we have shown that there exists a quantity \(X\) in the algebra

\[
\Sigma = (i^sj^r) \quad (s = 0, 1, \cdots, 5; r = 0, 1, 2),
\]
such that $X \neq 0$ and

$$\text{(67)} \quad (Xz)^2 = \lambda \text{ in } F.$$  

Suppose next that $a$ were zero so that from its origin (21) we have $s = 0$ and $h = 0$ in (17). Then (16) becomes

$$f'\gamma = (fz)^2 = 1,$$

while then obviously $f$ cannot be zero and $f = \alpha^{-1}r = \alpha^{-1}b_0$ is in $F(i)$ and in $\Sigma$. Again we have (67) for $X \neq 0$ in $\Sigma$. Finally the only remaining case is $b$ zero. Then $r_{a0} = 0$ so that $r = 0$ in (17), and hence the quantity $f$ is zero. Equation (16) now becomes $hh'\gamma = (hz)^2 = -1$, and since then $h = \alpha^{-1}s = a$ in $F(i)$ cannot be zero when $(hz)^2 = -1$, we have again proved the existence of $X \neq 0$ in $\Sigma$ and satisfying (67). Hence in all cases we have

**Lemma 4.** There exists a quantity $X$ in $\Sigma$ such that $X \neq 0$, and if $y = Xz$ then

$$\text{(68)} \quad y^2 = \lambda \text{ in } F.$$

The quantities $1, v, y, vy$ are linearly independent with respect to $F$, for otherwise (6) could not be a basis of $D$ when $X \neq 0$. A relation of the form

$$\xi_1 + \xi_2v + (\xi_3 + \xi_4)Xz = 0,$$

with $\xi_1, \xi_2, \xi_3, \xi_4$ not all zero and in $F$, would then evidently express $z$ as a quantity of $\Sigma$. Also $v^2 = \rho, y^2 = \lambda, vy = Xzv = -Xz = -vy$, since $v$, a polynomial in $i$ commutative with $j$, is commutative with $X$. But the linear set

$$\Gamma = (1, v; y, vy)$$

is evidently a generalized quaternion algebra over $F$, and is a normal division cyclic algebra over $F$. Hence $D$, containing $\Gamma$, is the direct product* of $\Gamma$ and another algebra $\Omega$ of order nine over $F$. Since $D$ is a normal algebra, so is necessarily $\Omega$,† so that $\Omega$ is a cyclic algebra‡ of order nine. Hence $D$, the direct product of algebra $\Gamma$ and algebra $\Omega$, is a cyclic algebra.§

**Theorem.** Every normal division algebra of type $R$ in thirty-six units is a cyclic algebra.

---


† For the first and second of the above references respectively see Theorems 7 and 16 of the author’s paper, *On direct products, cyclic division algebras, and pure Riemann matrices*, which appears in the present number of these Transactions.

‡ A theorem of Wedderburn, these Transactions, vol. 22 (1921), pp. 129–135.

COLUMBIA UNIVERSITY,
New York, N. Y.