References

1. N. Bourbaki, *Algèbre commutative*, Hermann, Paris, 1961.
2. H. Cartan and S. Eilenberg, *Homological algebra*, Princeton Univ. Press, Princeton, N. J., 1956.
3. M. Nagata, *Local rings*, Interscience, New York, 1962.
4. O. Zariski and P. Samuel, *Commutative algebra*, Vols. 1, 2, Van Nostrand, New York, 1958–1960.

New Mexico State University

ON ASSOCIATIVE DIVISION ALGEBRAS OF PRIME DEGREE[1]

A. A. ALBERT

In 1938 Richard Brauer showed[2] that, if $\mathfrak{D}$ is an associative division algebra of degree five over its center $\mathfrak{F}$, there is a field $\mathfrak{K}$ of degree at most twelve over $\mathfrak{F}$ such that the scalar extension $\mathfrak{D}\times\mathfrak{K}$ is a cyclic algebra over $\mathfrak{K}$. Indeed $\mathfrak{K}=\mathfrak{F}(\alpha_1, \alpha_2, \alpha_3)$, where α_1 is a root of a quadratic equation over $\mathfrak{F}$, α_2 is a root of a quadratic equation over $\mathfrak{F}(\alpha_1)$, and α_3 is a root of a cubic equation over $\mathfrak{F}(\alpha_1, \alpha_2)$. Since that time there has been no progress in the study of the structure of associative central division algebras of prime degree.

In view of Brauer's result it seems reasonable, as a first step in the study of central division algebras $\mathfrak{D}$ of prime degree p over $\mathfrak{F}$, to consider the case where there is a quadratic field $\mathfrak{K}$ over $\mathfrak{F}$ such that $\mathfrak{D}_{\mathfrak{K}}$ is cyclic. Then $\mathfrak{D}_{\mathfrak{K}}=\mathfrak{D}\times\mathfrak{K}$ has a subfield $\mathfrak{Z}$ which is cyclic of degree p over $\mathfrak{K}$. The simplest subcase is that where $\mathfrak{Z}$ is actually normal, but, of course, not cyclic over $\mathfrak{F}$. We shall treat this case under the assumption that $\mathfrak{F}$ has characteristic p, and shall prove that then $\mathfrak{D}$ is a cyclic algebra over $\mathfrak{F}$.

Our proof proceeds as follows. We are assuming that $\mathfrak{D}$ is a central division algebra of prime degree p over $\mathfrak{F}$ and that $\mathfrak{K}=\mathfrak{F}(t)$ is a quadratic extension of $\mathfrak{F}$. Let J be the automorphism of $\mathfrak{K}$ such that $tJ=-t$. Then we may extend J to an automorphism J of $\mathfrak{D}\times\mathfrak{K}$ such that $dJ=d$ for every d in $\mathfrak{D}$. We are also assuming that there is an element z in $\mathfrak{D}\times\mathfrak{K}$ such that the field $\mathfrak{Z}=\mathfrak{K}(z)$ is not only cyclic over

Received by the editors April 1, 1964.

[1] This paper was sponsored in part by the National Science Foundation under NSF Grant GP 2424.

[2] Proc. Nat. Acad. Sci. U. S. A. 24 (1938), 243–246.

$\mathfrak{K}$ but is actually *normal* over $\mathfrak{F}$. It may be assumed to be noncyclic since otherwise it has a cyclic subfield $\mathfrak{W}$ of degree p over $\mathfrak{F}$, and there is a scalar extension field of $\mathfrak{F}$ isomorphic to $\mathfrak{W}$ and which splits $\mathfrak{D}$. Then $\mathfrak{D}$ is a cyclic algebra over $\mathfrak{F}$. Hence $\mathfrak{Z}$ is a *bicyclic* field, and has an automorphism group generated by two automorphisms S and T such that

$$T^2 = S^p = I, \qquad TS = S^{-1}T, \tag{1}$$

where T induces J in $\mathfrak{K}$. The element z can always[3] be selected so that

$$z^p = z + k \qquad (k \text{ in } \mathfrak{K}) \tag{2}$$

and

$$zS = z + 1, \qquad tS = t, \qquad tT = -t. \tag{3}$$

The fixed field of $\mathfrak{Z}$ under T is a subfield $\mathfrak{W} = \mathfrak{F}(w)$ of degree p over $\mathfrak{F}$ which is *not* cyclic over $\mathfrak{F}$. It should now be clear that, if $\mathfrak{W}_0$ is a scalar extension $\mathfrak{F}(w_0)$ isomorphic to $\mathfrak{W}$, the field $\mathfrak{F}(w_0, t)$ is isomorphic over $\mathfrak{F}$ to $\mathfrak{Z}$ and splits $\mathfrak{D}\times\mathfrak{K}$. But then $\mathfrak{F}(w_0)$ must[4] split $\mathfrak{D}$. Hence there is an element w_1 in $\mathfrak{D}$ such that $\mathfrak{F}(w_1)$ is isomorphic to $\mathfrak{F}(w)$. Then $\mathfrak{F}(w_1, t) = \mathfrak{Z}_1$ is isomorphic over $\mathfrak{F}$ to $\mathfrak{Z}$. There is thus no loss of generality if we take $\mathfrak{Z}_1 = \mathfrak{Z}$ and so $w_1 = w$ is an element of $\mathfrak{D}$. Thus $w = wT = wJ$ and we may take the defining automorphism T of $\mathfrak{Z}$ to be induced by J. We state this result as follows.

LEMMA. *Let $\mathfrak{D}\times\mathfrak{K}$ have bicyclic splitting field of degree p over $\mathfrak{K}$. Then there is a normal subfield $\mathfrak{Z}$ of degree p over $\mathfrak{K}$ of $\mathfrak{D}\times\mathfrak{K}$ such that the automorphism J of $\mathfrak{K}$ may be extended to an automorphism J of $\mathfrak{D}\times\mathfrak{K}$ which leaves the elements of $\mathfrak{D}$ fixed and induces an automorphism J in $\mathfrak{Z}$. Then $\mathfrak{D}$ is the set of all elements d of $\mathfrak{D}\times\mathfrak{K}$ such that $d = dJ$.*

The algebra $\mathfrak{D}^* = \mathfrak{D}\times\mathfrak{K}$ is now a cyclic algebra[5]

$$(\mathfrak{Z}, S, g) = \mathfrak{Z} + \mathfrak{Z}y + \cdots + \mathfrak{Z}y^{p-1}, \tag{4}$$

where $\mathfrak{Z} = \mathfrak{K}(z)$ as above and

$$y^i x = xS^i y^i, \qquad y^p = g \qquad (i = 1, 2, \cdots, p-1), \tag{5}$$

for g in $\mathfrak{K}$. We also observe that, since we have selected z so that zJ

[3] For the theory of cyclic p-fields see p. 203 of the author's *Modern higher algebra*.

[4] For the extension of $\mathfrak{D}\times\mathfrak{F}[w_0]$ to $\mathfrak{D}\times\mathfrak{K}[w_0]$ is a total matric algebra. Since $\mathfrak{K}$ has degree two over $\mathfrak{F}$ the field $\mathfrak{K}[w_0]$ cannot split $\mathfrak{D}\times\mathfrak{F}[w_0]$ by Theorem 21 on p. 59 of the author's *Structure of algebras*. Hence $\mathfrak{D}\times\mathfrak{F}[w_0]$ must be split. Then Theorem 24 on p. 61 implies that $\mathfrak{F}[w_0]$ is isomorphic to a subfield of $\mathfrak{D}$.

[5] See pp. 74–75 of our *Structure of algebras* for this notation and related results.

is in $\mathfrak{Z}$ we have

$$(zJ)^p = zJ + kJ. \tag{6}$$

We assume, at this point, that $\mathfrak{F}$ has characteristic p. Then, since z and zJ are in the field $\mathfrak{Z}$, we have

$$(z + zJ)^p = (z + zJ) + (k + kJ). \tag{7}$$

If $z+zJ$ is not in $\mathfrak{F}$ it generates a field $\mathfrak{F}[w]$ of degree p over $\mathfrak{F}$. But then (7) implies that $\mathfrak{F}[w]$ is a cyclic field, and so $\mathfrak{D}$ is a cyclic algebra. Hence let $z+zJ=2\lambda$ where λ is in $\mathfrak{F}$. Then $(z-\lambda)J=(\lambda-z)$ and we can take $z'=z-\lambda$, $(z')^p=z^p-\lambda^p=z+k-\lambda+\lambda-\lambda^p=z'+k'$, $z'J=-z'$, $(z')^pJ=(z'J)^p=(-z')^p=-z'-k'=z'J+kJ$. Thus $k'J=-k'$. Hence we may always select z so that

$$zJ = -z, \qquad z^p = z + k, \qquad kJ = -k, \tag{8}$$

where k is in $\mathfrak{F}(t)$.

We now apply the automorphism J of $\mathfrak{D}^*$ to the case $i=1$ of the equation

$$y^iz = (z + i)y^i, \tag{9}$$

where (9) is a consequence of $yz=(zS)y=(z+1)y$. Then $(yz)J=yJzJ=-(yJ)z=[(z+1)y]J=(zJ+1)(yJ)=(1-z)yJ$, $(yJ)z=(z-1)(yJ)$, $(yJ)(z+1)=(yJ)z+yJ=(z-1)yJ+yJ=z(yJ)$. Hence

$$[(yJ)y]z = (yJ)(z + 1)y = z(yJy). \tag{10}$$

It follows that

$$yJy = d \tag{11}$$

is an element of $\mathfrak{Z}$. Thus $yJ=dy^{-1}$, and it follows that

$$(yJ)^p = gJ = N(d)g^{-1}, \tag{12}$$

where $N(d)=d(dS)\cdots(dS^{p-1})$ is the norm in $\mathfrak{Z}$ over $\mathfrak{R}$ of d and is in $\mathfrak{R}$. The integer $p=2q-1$ and, if

$$h = \left(\frac{g}{gJ}\right)^q, \tag{13}$$

then $h=g^qN(d)^{-q}g^q=g^{p+1}N(d^{-q})=gN(d^{-q}g)$. We replace y by $y^*=d^{-q}gy$ and have $h=(y^*)^p$ and $hJ=h^{-1}$. Thus there is no loss of generality if we assume that

$$gJ = g^{-1}. \tag{14}$$

We now take $v=y+y^{-1}$. Then $v^p=(y+y^{-1})^p=y^p+(y^{-1})^p=g+gJ$

is in $\mathfrak{F}$. Since v is not in $\mathfrak{F}$ we have proved that $\mathfrak{D}^*$ has a splitting field $\mathfrak{K}(\omega)$ where $\omega^p = g + gJ$ is in $\mathfrak{F}$. Then $\mathfrak{F}(\omega)$ must split $\mathfrak{D}$ and it is then known that $\mathfrak{D}$ is cyclic.

This completes our proof of the following result.

THEOREM. *Let $\mathfrak{D}$ be an associative division algebra of prime degree p over a center $\mathfrak{F}$ of characteristic p, and let there exist a quadratic extension field $\mathfrak{K}$ of $\mathfrak{F}$ such that $\mathfrak{D} \times \mathfrak{K}$ contains a subfield $\mathfrak{Z}$ of degree p over $\mathfrak{K}$ which is normal over $\mathfrak{F}$. Then $\mathfrak{D}$ is a cyclic algebra over $\mathfrak{F}$.*

It is interesting to note that in fact $yz = (z+1)y$ and $y^{-1}z = (z-1)y^{-1}$ implies that if

$$u = z(y + y^{-1})(y - y^{-1})^{-1}$$

then $(y+y^{-1})z = (z+1)y + (z-1)y^{-1} = z(y+y^{-1}) + (y-y^{-1})$ and so $(y+y^{-1})u = z(y+y^{-1})(y+y^{-1})(y-y^{-1})^{-1} + (y+y^{-1}) = (u+1)(y+y^{-1})$. Also $u^p = u + \alpha$ where $\alpha = \Delta(u)$ is the norm of u in the algebra $\mathfrak{D} \times \mathfrak{K}$. Since Δ is a multiplicative function we have

$$\Delta(u) = \Delta(z)\Delta(y + y^{-1})[\Delta(y - y^{-1})]^{-1} = k(g + gJ)(g - gJ)^{-1},$$

where $k = -kJ$ and $g - gJ = -(g - gJ)J$ so that α is in $\mathfrak{F}$. Thus $\mathfrak{D}$ is isomorphic to $\mathfrak{B} + \mathfrak{B}v + \cdots + \mathfrak{B}v^{p-1}$ where $\mathfrak{B} = \mathfrak{F}(u)$, $u^p = u + \alpha$, $v^p = b + gJ = \gamma$ for α and γ in $\mathfrak{F}$.

UNIVERSITY OF CHICAGO