CYCLICITY OF DIVISION ALGEBRAS OF PRIME DEGREE

SAM PERLIS

It is not known whether a central division algebra D of prime degree p over a field F can be noncyclic. Every such algebra which has been constructed is cyclic and, when any of various mild conditions is imposed on D, it can be proved that D is cyclic.

We consider only the case in which the characteristic of D is equal to its degree p. For this case, it is known[1] that cyclicity of D is guaranteed by the following conditions: there is an extension field K of F such that

(i) K/F has degree m with $(m, p)=1$;

(ii) D_K is cyclic with maximal subfield W which is galois over F;

(iii) K/F is cyclic.

We shall prove:

THEOREM. *Cyclicity of D is implied by conditions* (i) *and* (ii) *together with*

(iii′) *K/F is galois.*

Our proof of the theorem is a reduction to the case in which the result of AAA applies. It should be noted however that the proof given in AAA can be generalized[2] to provide the present theorem directly.

COROLLARY. *Cyclicity of D is implied by* (ii) *and the condition that K/F is separable of degree $m<p$.*

For proof of the corollary, let L be the normal closure of K/F. Then L/F has degree n prime to p. The algebra D_L is cyclic with WL as a maximal subfield which is galois over F. The theorem then states that D is cyclic.

Throughout, we adhere to the notations of this introduction.

For any galois extension L of a field M, let $G(L/M)$ denote the automorphism group of L/M. We let

Received by the editors March 25, 1968 and, in revised form, June 28, 1968.

[1] A. A. Albert, *A note on normal division algebras of prime degree*, Bull. Amer. Math. Soc. **44** (1938), 649–652. This paper is referred to herein as AAA.

[2] In its first version, this paper generalized the proof of AAA. Credit is due the referee for pointing out that the first version contained the apparatus and ideas for the simpler proof by reduction presented here.

$$\mathfrak{G} = G(W/F), \qquad \mathfrak{K} = G(W/K)$$

so that $\mathfrak{K}$ is normal in $\mathfrak{G}$, $\mathfrak{K}$ has order p, and $\mathfrak{G}$ has order mp. Since W/K is galois of prime degree, it is cyclic and $\mathfrak{K} = \langle S \rangle$ is a cyclic group generated by an automorphism S. Now $\mathfrak{G}$ is an extension of a commutative group $\mathfrak{K}$ by a group $\mathfrak{Q} = \mathfrak{G}/\mathfrak{K}$ of order relatively prime to that of $\mathfrak{K}$. In this circumstance $\mathfrak{G}$ is known[3] to contain a subgroup $\mathfrak{I}$ of order m and be a semidirect product of $\mathfrak{K}$ by $\mathfrak{I}$:

$$\mathfrak{G} = \mathfrak{K} \times_\alpha \mathfrak{I} = \{TS^i;\ i = 0, \cdots, p-1,\ T \in \mathfrak{I}\}, \quad T^{-1}ST = S^e.$$

Here e depends on T and α denotes a homomorphism from $\mathfrak{I}$ into the group aut $\mathfrak{K}$ of automorphisms of $\mathfrak{K}$; for each $T \in \mathfrak{I}$ the image $T\alpha$ is the automorphism $S \to S^e$ determined by the residue class modulo p of the integer e.

The kernel of α is the set $\mathfrak{I}_0 = \mathfrak{I}_0(\alpha)$ of all $T \in \mathfrak{I}$ which commute with S, i.e., the $\mathfrak{I}$-centralizer of $\mathfrak{K}$. Since $\mathfrak{I}/\mathfrak{I}_0$ is isomorphic to a subgroup of aut $\mathfrak{K}$, and the latter is isomorphic to the multiplicative group of integers modulo p, which is cyclic, we have

LEMMA. *If $\mathfrak{I}_0 = \mathfrak{I}_0(\alpha)$ denotes the $\mathfrak{I}$-centralizer of $\mathfrak{K}$, then $\mathfrak{I}/\mathfrak{I}_0$ is cyclic.*

The subgroup $\mathfrak{I}$ of $\mathfrak{G} = \mathfrak{K} \times_\alpha \mathfrak{I}$ corresponds to a fixed subfield Z of degree p over F,

$$\mathfrak{I} = G(W/Z), \qquad [Z:F] = p.$$

Since the degrees of K and Z over F are relatively prime, W is the join of these fields,

$$W = ZK = Z \otimes_F K.$$

The automorphism group of K/F is isomorphic to $\mathfrak{G}/\mathfrak{K} \cong \mathfrak{I}$ and is simply the restriction $\mathfrak{I}_K$ of $\mathfrak{I}$ to K. There is no harm, therefore, if we write $\mathfrak{I}$ for $\mathfrak{I}_K$ and thus regard $\mathfrak{I}$ as a group of automorphisms of K which become automorphisms of $W = ZK$ when each $T \in \mathfrak{I}$ is taken to be the identity on Z.

Let W_0 be the field between W and Z such that $\mathfrak{I}_0 = G(W/W_0)$. When $\mathfrak{I}$ is regarded as $G(K/F)$, the subgroup $\mathfrak{I}_0$ corresponds to a fixed field K_0 between K and F, and we shall see that

$$W_0 = ZK_0 = Z \otimes_F K_0.$$

---

[3] By the Schur-Zassenhaus lemma. Cf. J. J. Rotman, *The theory of groups*, Allyn and Bacon, Boston, Mass., 1965, p. 145.

First, $\mathfrak{J}_0$ fixes each element of Z and each of K_0 so that $\mathfrak{J}_0$ fixes all of ZK_0. Thus $W_0 \supseteq ZK_0$. But

$$\text{order of } \mathfrak{J}_0 = m_0 = [W: W_0] = [K: K_0].$$

Since the degrees of Z and K_0 over F are p and m/m_0, which are relatively prime, we have

$$[ZK_0: F] = pm/m_0 = [W_0: F].$$

Thus, $W_0 = ZK_0 = Z \otimes_F K_0$.

Since $\mathfrak{J}_0 = G(W/W_0)$ is normal in $\mathfrak{J} = G(W/Z)$ with cyclic quotient group, it follows that W_0/Z is cyclic. Since W is a splitting field (this term always being used in the sense of isomorphism) for D, and the degree m_0 of W/W_0 is prime to the degree p of D, it follows[4] that W_0 is a splitting field for D. Now $W_0 \supset K_0$ and the algebra D_{K_0} has $W_0 = ZK_0$ as a splitting field. We shall see next that (a) K_0/F is cyclic and (b) W_0/K_0 is cyclic, W_0/F is galois.

The subgroup $\mathfrak{J}_0$ is normal in $\mathfrak{J}$ and commutes elementwise with $\mathfrak{K} = \langle S \rangle$, and therefore $\mathfrak{J}_0$ is normal in $\mathfrak{G}$. Hence W_0/F is galois and so is W_0/K_0. But the latter has degree p, hence is cyclic, and this is (b). When we take $\mathfrak{J} = G(K/F)$, $\mathfrak{J}_0 = G(K/K_0)$ we find that the group of K_0/F is isomorphic to the cyclic group $\mathfrak{J}/\mathfrak{J}_0$, thus obtaining (a).

Now we may see that the theorem of AAA applies to D and its scalar extension D_{K_0}. For, K_0 is cyclic over F of degree prime to p, and D_{K_0} has a splitting field W_0 which is galois over F and cyclic of degree p over K_0. It follows from AAA that D is cyclic.

PURDUE UNIVERSITY

[4] A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloq. Publ., Vol. 24, Amer. Math. Soc., Providence, R. I., 1964, Theorem 20, p. 59.