PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 131, Number 12, Pages 3673–3676
S 0002-9939(03)06959-4
Article electronically published on February 26, 2003

CYCLICITY CONDITIONS FOR DIVISION ALGEBRAS OF PRIME DEGREE

M. MAHDAVI-HEZAVEHI AND J.-P. TIGNOL

(Communicated by Martin Lorenz)

ABSTRACT. Let D be a division algebra of prime degree p. A set of criteria is given for cyclicity of D in terms of subgroups of the multiplicative group D^* of D. It is essentially shown that D is cyclic if and only if D^* contains a nonabelian metabelian subgroup.

The multiplicative group of a noncommutative division ring has been investigated in various papers by Hua [4], [5], Scott [8], Herstein [3], Amitsur [1], and Huzurbazar [6]. For some recent results see [7]. In this note we concentrate on the case of division algebras of prime degree.

Let D be a division algebra with center F and degree p (i.e., $\dim_F D = p^2$), with p prime. The algebra D is called *cyclic* if it contains a cyclic extension of F of degree p. It is known that division algebras of degree $p = 2, 3$ are cyclic; the existence of noncyclic division algebras of prime degree $p \geq 5$ is unknown. If K is a cyclic extension of degree p of F in D, then the Skolem–Noether theorem yields an element z such that the inner automorphism $x \mapsto zxz^{-1}$ restricts to a nontrivial automorphism of K and $z^p \in F^*$; see [2, p. 49]. In particular, zF^* is an element of order p in D^*/F^*. Conversely, a theorem of Albert (see [2, p. 87]) asserts that D is cyclic if D^*/F^* contains an element of order p. The object of this note is to give further equivalent cyclicity conditions in terms of the groups D^* and D^*/F^*.

Our main result is the following:

Theorem. *Let D be a central division F-algebra of prime degree p. The following conditions are equivalent:*

(a) *D is cyclic;*
(b) *D^* contains a nonabelian soluble subgroup;*
(c) *D^* contains a nonabelian metabelian subgroup;*
(d) *D^*/F^* contains a nontrivial finite subgroup;*
(e) *D^*/F^* contains an element of order p;*
(f) *D^*/F^* contains a nonabelian soluble subgroup;*
(g) *D^*/F^* contains a nonabelian metabelian subgroup.*

Received by the editors June 19, 2002 and, in revised form, July 15, 2002.
2000 *Mathematics Subject Classification.* Primary 16K20.
The first author thanks the Research Council of Sharif University of Technology for support. He also thanks Professor J.-P. Tignol for his hospitality during his stay at the Université Catholique de Louvain in May 2002.
The second author was partially supported by the National Fund for Scientific Research (Belgium).

The main ingredient in the proof of $(b) \Rightarrow (a)$ is the following:

Lemma. *Using the same notation as in the Theorem, suppose $T \subset D^*$ is a nonabelian soluble subgroup containing F^*. If T/F^* is infinite, then there is a cyclic extension K/F such that T lies in the normalizer $N_{D^*}(K^*)$ of K^*.*

Proof of the Lemma. By [7, Lemma 3], we may find an abelian normal subgroup $A \subset T$ of finite index. Take A maximal. We have $A \subset AF^* \subset T$, and $AF^* \neq T$ since T is nonabelian. By maximality of A we conclude that $A = AF^*$, hence $F^* \subseteq A$. Since T/F^* is infinite, we have $F^* \neq A$. The subfield $K = F(A)$ is then maximal in D. Since A is normal in T we have $T \subset N_{D^*}(K^*)$. On the other hand, $T \not\subset K^*$ since T is nonabelian. Let $z \in T \setminus K^*$. Then the inner automorphism obtained from z restricts on K to a nontrivial automorphism of K/F. Therefore, K/F is cyclic, and this completes the proof of the Lemma. □

Proof of the Theorem. The implications $(a) \Rightarrow (e) \Rightarrow (d)$, $(g) \Rightarrow (f) \Rightarrow (b)$, and $(c) \Rightarrow (b)$ are clear.

$(a) \Rightarrow (c)$, (g). Let $K \subset D$ be a maximal subfield such that K/F is cyclic. Consider the normalizer $N = N_{D^*}(K^*)$ of K^* in D^*. We have $N/K^* \cong \mathrm{Gal}(K/F) \cong \mathbb{Z}/p\mathbb{Z}$, hence N is a metabelian subgroup of D^*. If $u_1, \ldots, u_p$ is a normal basis of K/F, we may find $v \in N$ such that $vu_1v^{-1} = u_2$, hence $vu_1 \not\equiv u_1v \bmod F^*$. This shows N/F^* (hence also N) is not abelian, so (c) and (g) follow.

$(d) \Rightarrow (a)$. Let $T/F^* \subset D^*/F^*$ be a nontrivial finite subgroup and denote by D^1 the kernel of the reduced norm map $\mathrm{Nrd}\colon D^* \to F^*$. Two cases may occur:

- If $T \cap D^1 \subset F^*$, then for $x \in T \setminus F^*$ we have $x^p/\mathrm{Nrd}(x) \in T \cap D^1 \subset F^*$. Thus, by Albert's criterion (see [2, p. 87]), D is cyclic.
- If $T \cap D^1 \not\subset F^*$, pick an element $x \in T \cap D^1 \setminus F^*$, so $F(x) \neq F$. Since T/F^* is finite we have $x^n \in F^*$ for some integer $n \neq 0$. Set $x^n = a$. Taking the reduced norm of both sides of the last equation we obtain $1 = a^p$ and hence $x^{np} = 1$. Let m be the smallest integer such that $x^m = 1$. Then, m is not divisible by the characteristic of F, and $F(x)$ may be identified with the field $F(\mu_m)$ of m-th roots of unity. It follows that $F(x)/F$ is Galois, hence (a) is proved.

$(b) \Rightarrow (a)$. Let $S \subset D^*$ be a nonabelian soluble subgroup and set $T = SF^*$. Then T is also nonabelian soluble. If T/F^* is infinite, then the Lemma yields (a). If T/F^* is finite, then we have (d), hence also (a) since $(d) \Rightarrow (a)$ has been proved above.

The proof of the Theorem is thus complete. □

We conclude with a few observations on the case where F contains all the roots of unity of order prime to the characteristic. This hypothesis imposes severe restrictions on subgroups of D^*/F^*:

Corollary. *If F contains all the roots of unity of order prime to the characteristic, then every nontrivial finite subgroup of D^*/F^* (if any) is cyclic of order p or elementary abelian of order p^2.*

Proof. Let T/F^* be a nontrivial finite subgroup of D^*/F^*. In view of the hypothesis on F, the proof of $(d) \Rightarrow (a)$ above shows that $T \cap D^1 \subset F^*$, and that $x^p\,\mathrm{Nrd}(x)^{-1} \in$

F^* for all $x \in T$. Since the derived group T' is in D^1, it follows that T/F^* is abelian and p-torsion, hence it is elementary abelian of exponent p. If $x_1, \ldots, x_r \in T$ have distinct images in T/F^*, it is easily seen that $x_1, \ldots, x_r$ are linearly independent over F (see [9, p. 130]). Therefore, the order of T/F^* is at most p^2. □

In contrast with the Theorem, the group D^1 of reduced norm 1 elements (or, equivalently, the derived group D' since $D' = D^1$ by [2, Theorem 4, p. 164]) does not contain any nonabelian soluble subgroup when F satisfies the hypothesis in the Corollary above.

Proposition. *Using the same notation as in the Theorem, if F contains all the roots of unity of order prime to the characteristic, then the group D^1 does not contain any nonabelian soluble subgroup.*

Proof. Suppose $S \subset D^1$ is a nonabelian soluble subgroup and let $T = SF^*$. As a first step in the proof, we show that there is a maximal subfield $K \subset D$ such that K/F is cyclic and $S \subset T \subset N_{D^*}(K^*)$. This readily follows from the Lemma if T/F^* is infinite.

If T/F^* is cyclic, then T (hence also S) is abelian, a contradiction.

If T/F^* is elementary abelian of order p^2, let $x \in T \setminus F^*$ and let $y \in T$ be an element which does not commute with x. We have $yxy^{-1} \in xF^*$ since T/F^* is abelian, hence the inner automorphism obtained from y induces a nontrivial automorphism of $F(x)$. Therefore, $F(x)/F$ is a cyclic extension of F. Since T/F^* is generated by the images of x and y, it follows that T lies in the normalizer of $F(x)^*$.

The Corollary shows that the two cases above exhaust all the possibilities for T/F^* when it is finite. Therefore, we may always find a maximal subfield $K \subset D$ with K/F cyclic and $S \subset T \subset N_{D^*}(K^*)$. Pick $z \in D^*$ such that the inner automorphism obtained from z restricts to a nontrivial automorphism of K/F and let $z^p = a \in F^*$. Then

$$N_{D^*}(K^*) = K^* \cup K^*z \cup \cdots \cup K^*z^{p-1}.$$

Since S is not abelian, we must have $S \not\subset K^*$; hence $kz^i \in S$ for some $k \in K^*$ and some integer i with $1 \leq i \leq p-1$. Since $S \subset D^1$, it follows that $\mathrm{Nrd}(kz^i) = 1$, hence

$$N_{K/F}(k) = \begin{cases} a^{-i} & \text{if } p \text{ is odd,} \\ -a^{-1} & \text{if } p = 2. \end{cases}$$

Therefore, in both cases a is a norm from the extension K/F: if p is odd this is because i is prime to p, and if $p = 2$ this is because -1 is a square in F by hypothesis. By [2, p. 73], it follows that D is not a division algebra, a contradiction. □

Example. The Corollary and the Proposition do not hold without hypothesis on F, as the following example shows. Let $D = (-3, -1)_{\mathbb{Q}}$ be the quaternion algebra with basis 1, i, j, ij such that $i^2 = -3$, $j^2 = -1$, and $ji = -ij$ over the field $\mathbb{Q}$ of rational numbers. Then $\omega = (-1 + i)/2 \in D$ has order 3 and reduced norm 1. Now, ω and j generate a subgroup of D^1 which is a generalized quaternion group of order 12 (and their images in D^*/F^* generate a subgroup isomorphic to S_3, the symmetric group on three elements).

References

1. S. A. Amitsur, Finite subgroups of division rings, *Trans. Amer. Math. Soc.*, **80** (1955), 361–386. MR **17:**577c
2. P. K. Draxl, Skew fields, LMS Lecture Note Series, No. 81, Cambridge University Press, (1982). MR **85a:**16022
3. I. N. Herstein, Finite multiplicative subgroups in division rings, *Pacific J. Math.* **3** (1953), 121–126. MR **14:**1056j
4. Hua Loo-Keng, Some properties of a field, *Proc. Nat. Acad. Sci. U.S.A.* **35** (1949), 533–537. MR **11:**155c
5. Hua Loo-Keng, On the multiplicative group of a field, *Acad. Sinica Science Record* **3** (1950), 1–6 (English, Chinese summary). MR **12:**584e
6. M. S. Huzurbazar, The multiplicative group of a division ring, *Dokl. Akad. Nauk SSSR* **131** (1960), 1268–1271 = *Soviet Math. Dokl.* **1** (1960), 433–435. MR **22:**11009
7. M. Mahdavi-Hezavehi, Free subgroups in maximal subgroups of $GL_1(D)$, *J. Algebra* **241** (2001), 720–730. MR **2002c:**16023
8. W. R. Scott, On the multiplicative group of a division ring, *Proc. Amer. Math. Soc.* **8** (1957), 303–305. MR **18:**788g
9. J.-P. Tignol, Sur les décompositions des algèbres à division en produit tensoriel d'algèbres cycliques, in *Brauer groups in ring theory and algebraic geometry* (F. van Oystaeyen and A. Verschoren, eds), Lecture Notes in Math. 917, Springer-Verlag, Berlin, 1982, pp. 126–145. MR **83i:**16020

Department of Mathematical Sciences, Sharif University of Technology, P. O. Box 11365–9415, Tehran, Iran

E-mail address: mahdavih@sharif.edu

Institut de Mathématique Pure et Appliquée, Université Catholique de Louvain, 1348 Louvain-la-Neuve, Belgium

E-mail address: tignol@math.ucl.ac.be