Crossed Product Conditions for Division Algebras of Prime Power Degree

D. Kiani, M. Mahdavi-Hezavehi
kiani@mehr.sharif.edu
mahdavih@sharif.edu
Department of Mathematical Sciences
Sharif University of Technology
P. O. Box 11365-9415
Tehran, Iran

Abstract

Let D be an F-central division algebra of degree p^r, p a prime. A set of criteria is given for D to be a crossed product in terms of irreducible soluble or abelian-by-finite subgroups of the multiplicative group D^* of D. Using the Amitsur's classification of finite subgroups of D^* and the Tits Alternative, it is shown that D is a crossed product if and only if D^* contains an irreducible soluble subgroup. Further criteria are also presented in terms of irreducible abelian-by-finite subgroups and irreducible subgroups satisfying a group identity. Using the above results, it is shown that if D^* contains an irreducible finite subgroup, then D is a crossed product.

1 Introduction

Let D be an F-central division algebra of degree n. The algebra D is called a *crossed product* if it contains a maximal subfield K such that K/F is Galois. We shall say that D is a *nilpotent* crossed product if $Gal(K/F)$ is nilpotent. A subgroup G of D^*

is said to be *irreducible* if $F[G] = D$. When $n = p$, a prime, it is shown in [6] that D is cyclic if and only if D^* contains a nonabelian soluble subgroup. A criterion is also given in [3] for D to be a supersoluble (nilpotent) crossed product division algebra in terms of subgroups D^*. More precisely, it is shown that D is a supersoluble (nilpotent) crossed product if and only if D^* contains an abelian-by-supersoluble (abelian-by-nilpotent) irreducible subgroup. The aim of this paper is to generalize some of these results to a division algebra of a prime power degree p^r. In fact, we present a set of criteria for D to be a crossed product in terms of irreducible soluble or abelian-by-finite subgroups of D^*. To be more precise, it is shown that D is a nilpotent crossed product if and only if D^* contains an irreducible soluble subgroup. In addition, it is shown that, except for the case $Char F = 0$, $p = 2$ and $r > 1$, D is a crossed product if and only if either of the following conditions holds: (i) D^* contains an irreducible abelian-by-finite subgroup, or (ii) D^* contains an irreducible subgroup satisfying a group identity. Furthermore, it is proved that these conclusions also hold for the above excluded case provided that D^* contains no finite subgroup isomorphic to $SL_2(Z_5)$. Finally, given a non-commutative F-central division algebra D of index p^r, p a prime, using the above mentioned results, it is shown that if D^* contains an irreducible finite subgroup G, then D is a crossed product. We note that soluble subgroups of the multiplicative group of a division ring were first studied by Suprunenko in [10].

2 Notations and conventions

We now recall some notations and conventions that are used throughout. Let D be an F-central division algebra and G be a subgroup of D^*. The F-linear hull of G, i.e., the F-algebra generated by elements of G over F, is denoted by $F[G]$. G is called *irreducible* if $D = F[G]$. For any group G we denote its center by $Z(G)$. Given a subgroup H of G, $N_G(H)$ means the *normalizer* of H in G, and $\langle H, K\rangle$ the group generated by H and K, where K is a subgroup of G. We shall say that H is *abelian-by-finite* if there is an abelian normal subgroup K of H such that H/K is finite. Let S be a subset of D, then the *centralizer* of S in D is denoted by $C_D(S)$. For notations and results, used in the text, on central simple algebras see [7].

3 Irreducible soluble subgroups

Let D be an F-central division algebra of degree p^r, p a prime. This section investigates the structure of D under the condition that D^* has an irreducible soluble subgroup. To be more precise, it is shown that D is a crossed product if and only if D^* contains an irreducible soluble subgroup. We begin our study with the following:

Lemma 1. *Let D be a finite dimensional F-central division algebra. If D is a soluble crossed product, then D^* contains an irreducible soluble subgroup.*

PROOF. Let K be a maximal subfield of D such that K/F is soluble Galois. By Skolem-Noether Theorem, for any $\sigma \in Gal(K/F)$ there exists an element $x \in N = N_{D^*}(K^*)$ such that $\sigma(k) = xkx^{-1}$, for all $k \in K$. Hence $N_{D^*}(K^*)/C_{D^*}(K^*) \simeq Gal(K/F)$. Since K is a maximal subfield of D, we have $C_{D^*}(K^*) = K^*$. Therefore, $N_{D^*}(K^*)$ is a soluble subgroup of D^*. To complete the proof of the lemma, it is enough to show that N is irreducible, i.e., $F[N] = D$. Put $D_1 = F[N]$. We have $C_D(D_1) \subseteq C_D(K) = K$, and hence $C_D(D_1)$ is an intermediate field of the Galois extension K/F. By the fact that every element of $Gal(K/F)$ is the restriction of an inner automorphism of N we conclude that $C_D(D_1) \subseteq Fix(Gal(K/F))$. Therefore $C_D(D_1) = F$. Now, by Centralizer Theorem, we obtain $D = C_D(F) = C_D(C_D(D_1)) = D_1$, which completes the proof. □

The following lemma is used in many proofs below, its idea is due to Suprunenko [10].

Lemma 2. *Let D be a finite dimensional F-central division algebra. Suppose that G is a subgroup of D^* such that $F^* \subseteq Z(G)$. If $K = Z(G) \cup \{0\}$ is a subfield of D and G/K^* is abelian, then we have $[K[G] : K] = |G/K^*|$ and hence G/K^* is a finite group.*

PROOF. Let $g_1, \ldots, g_t$ be a set of linearly independent elements of G over K. It is clearly seen that $g_1K^*, \ldots, g_tK^*$ are distinct elements of G/K^*. On the other hand, if $g_1K^*, \ldots, g_tK^*$ are distinct elements of G/K^*, we shall show that $g_1, \ldots, g_t$

are linearly independent over K. To see this, since G/K^* is abelian, for every $g \in G$ we have $gg_ig^{-1} = k_ig_i$ with $1 \leq i \leq t$, where $k_i \in K^*$. We claim that for each pair $i \neq j$ we can find an element g in G such that $k_i \neq k_j$. For suppose that for each g in G we have $gg_ig^{-1}g_i^{-1} = k_i = gg_jg^{-1}g_j^{-1} = k_j$. Therefore, we conclude that $[g, g_j^{-1}g_i] = 1$, and hence $g_j^{-1}g_i \in K^*$. This contradicts the choice of $g_i's$, and so the claim is established. Now, suppose that $g_1, \dots, g_t$ are linearly dependent over K and consider a relation

$$\lambda_1 g_1 + \ldots + \lambda_t g_t = 0. \qquad (*)$$

Of all relations of the form $(*)$, there must be at least one for which the number of nonzero terms is least. Let $(*)$ be such a relation. Now, we may assume that $\lambda_1 \neq 0, \lambda_2 \neq 0$ and choose g in G such that $k_1 = gg_1g^{-1}g_1^{-1} \neq gg_2g^{-1}g_2^{-1} = k_2$. From the relation $(*)$ we obtain
$k_1(\lambda_1 g_1 + \ldots + \lambda_t g_t) - g(\lambda_1 g_1 + \ldots + \lambda_t g_t)g^{-1} = \lambda_1 k_1 g_1 + \ldots \lambda_t k_1 g_t - (\lambda_1 k_1 g_1 + \ldots \lambda_t k_t g_t) = \lambda_2(k_1 - k_2)g_2 + \ldots + \lambda_t(k_1 - k_t)g_t = 0$.
Now, the last equation contradicts the choice of the relation $(*)$. Therefore, $g_1, \dots, g_t$ are a linearly independent subset of G over K, and this completes the proof.

To prove our next lemma, we shall need the following results from [3].

LEMMA A. *Let D be a finite dimensional F-central division algebra. Suppose that K is a subfield of D containing F. If G is an irreducible subgroup of D^* such that $K^* \lhd G$, then K/F is Galois and $G/C_G(K^*) \simeq Gal(K/F)$.*

LEMMA B. *Let D be a finite dimensional F-central division algebra and let G be an irreducible subgroup of D^*. If K is a subfield of D containing F such that $[G : C_G(K^*)] = [K : F]$, then $C_D(K) = F[C_G(K^*)]$.*

THEOREM C. *Let D be a noncommutative finite dimensional F-central division algebra. Then D is a nilpotent crossed product if and only if there exist an irreducible subgroup G of D^* and an abelian normal subgroup A of G such that G/A is nilpotent.*

Lemma 3. *Let D be a finite dimensional F-central division algebra of index n. Assume that D^* contains an irreducible soluble subgroup. Then we have the following:*
(i) there is an irreducible soluble subgroup G and a maximal abelian normal subgroup

K^* of G such that $K = K^* \cup \{0\}$ is a subfield of D and G/K^* is finite. Furthermore, setting $H := C_G(K^*)$, then the derived group H' of H is also finite.
(ii) Assume the notation of (i). If H' is abelian and $n = q^r$, q a prime, then G/K^* is a q-group.
(iii) Keep the notation of (i). If H' is nonabelian and $n = q^r$, q a prime, then H^{t-2} is a q-group, where H^i denotes the i-th term of the derived series of H.
(iv) If D is a non-crossed product with index $i(D) = 2^r$, then D^* contains the finite quaternion subgroup Q_8, or $SL_2(Z_3)$, or the binary octahedral group of order 48.

Proof. (i) Let G_0 be an irreducible soluble subgroup of D^*. By Lemma 3 of [5], we know that G_0 is abelian-by-finite, i.e., there is an abelian normal subgroup A in G_0 of finite index. Take A maximal in G_0, and set $K = F(A)$. One may easily show that $G_0 \subseteq N_{D^*}(A)$ and that K^*G_0 is an irreducible soluble subgroup of D^*. Set $G = K^*G$. Then, it is easily seen that K^* is maximal abelian normal in G and G/K^* is a finite group. Furthermore, we know that $H/Z(H)$ is finite and hence, by Theorem 15.1.13 of [8], the derived group H' is a finite group.

(ii) Because $H' \subseteq C_G(K^*)$, K^*H' is an abelian normal subgroup of G. Hence, by maximality of K^*, we have $H' \subseteq K^* = Z(H)$. Therefore, H/K^* is abelian. Now, by Lemma 2, we conclude that $[K[H] : K] = |H/K^*|$. Since $[D : F] = q^{2r}$ and $F^* \subseteq K^*$ we conclude that $[K[H] : K]$ divides q^{2r}, i.e., there exists a natural number s such that $|H/K^*| = [K[H] : K] = q^s$. Now, by Lemma A, we have $G/H \simeq Gal(K/F)$ and K/F is a Galois extension. Since $i(D) = q^r$ there exists a natural number t such that $|Gal(K/F)| = [K : F] = q^t$. Thus, $|G/H| = q^t$ and hence $|G/K^*| = q^{s+t}$, i.e., G/K^* is a q-group.

(iii) Suppose that H' is nonabelian. Then, the soluble length of H is $t = l(H) \geq 3$. Now, consider the derived chain $\langle e\rangle = H^t \subset H^{t-1} \subset \ldots \subset H' \subset H$. It is clear that H^{t-1} is abelian and H^{t-2} is a nonabelian subgroup of H'. Now, we know that $H^{t-1} \lhd G$ and $H^{t-1} \subset C_G(K^*)$. Thus, $H^{t-1}K^*$ is an abelian normal subgroup of G. Hence, by maximality of K^*, we conclude that $H^{t-1} \subseteq K^*$. Therefore, $H^{t-2}K^*/K^*$ is an abelian subgroup of G/K^*. Set $N = H^{t-2}K^*$. We note that N is normal in G, and hence $Z(N)$ is an abelian normal subgroup of G containing K^*. By maximality of K^*, we have $Z(N) = K^*$. Now, N is a subgroup of D^* such that N/K^* is abelian and $Z(N) = K^*$. By Lemma 2, we obtain $[K[N] : K] = |N/K^*|$. By our assumption, we know that $[K[N] : K]$ divides q^{2r}. Therefore, $N/K^* \simeq H^{t-2}/K^* \cap H^{t-2}$ is a q-group. Now, by Lemma B, we have $F[H] = K[H] = C_D(K)$. Put $D_1 = C_D(K)$. We know that $Z(D_1) = K$. We now claim that H^{t-2} is a q-group. To see this, let $x \in H^{t-2}$. Then, there exists a natural number s such that $x^{q^s} \in K^* \cap H^{t-2}$. On the other hand, $x^{q^s} \in H' \subset D_1'$, and hence $RN_{D_1/K}(x^{q^s}) = 1$. Since $x^{q^s} \in K^* = Z(D_1)^*$ we obtain $RN_{D_1/K}(x^{q^s}) = (x^{q^s})^{i(D_1)} = x^{q^{s+u}}$, where $i(D_1) = q^u$. Therefore, $x^{q^{s+u}} = 1$ and so H^{t-2} is a finite q-group.

(iv) Let G be the irreducible soluble subgroup obtained by (i) and keep the notations of the above cases. If H' is abelian, then by the case (ii), G/K^* is a 2-group and hence nilpotent and so G is an irreducible abelian-by-nilpotent subgroup of D^*. Now, by Theorem C, we conclude that D is a nilpotent crossed product, which contradicts our assumption that D is a non-crossed product. Therefore, H' is nonabelian. By (iii) we conclude that H^{t-2} is a finite 2-group. Now, by a result of [9, p.45], we conclude that H^{t-2} is cyclic or a (generalized) quaternion group. Since H^{t-2} is nonabelian we conclude that H^{t-2} is a (generalized) quaternion group. We recall that the (generalized) quaternion group of order 2^u, $u \geq 3$, is defined with the presentation $Q_{2^u} = \langle\ x, y \mid x^{2^{u-2}} = y^2,\ y^4 = 1,\ yxy^{-1} = x^{-1}\rangle$. It is clear that $\langle x\rangle \lhd Q_{2^u}$ and $Q_{2^u}^{(2)} = \langle x^2\rangle$. Thus, $\langle x^2\rangle$ is a characteristic subgroup of H^{t-2} and hence $\langle x^2\rangle$ is an abelian normal subgroup of G. We note that $\langle x^2\rangle \subset C_G(K^*)$ and so $K^*\langle x^2\rangle$ is an abelian normal subgroup of G. Therefore, by maximality of K^*, we have $\langle x^2\rangle \subset K^*$. Thus, $x^2 \in Z(Q_{2^u})$, and hence $x^{-2} = yx^2y^{-1} = x^2$. Therefore, $x^4 = 1$. On the other hand, we have $x^{2^{u-1}} = 1$, and so $u = 3$, i.e., $H^{t-2} \simeq Q_8$. Now, assume that N is a maximal normal 2-subgroup of H'. For every $g \in G$, set $N_1 = gNg^{-1}$. N_1 is a normal 2-subgroup of H'. Hence NN_1 is a normal 2-subgroup of H'. By maximality of N, we obtain $N_1 \subseteq N$ and so we have $N \lhd G$. We note that H' is finite and hence N is a finite 2-group. Thus, as in the case of H^{t-2} above, we conclude that $N \simeq Q_8$. Therefore, by a result of [9, p.54], we have either $H' \simeq Q_8 \times M$, where M is a group of odd order, or $H' \simeq SL_2(Z_3) \times M$, where M is a group of order m coprime to 6, or H' is isomorphic to the binary octahedral group. In the first case, M is a characteristic subgroup of H'. Therefore, M is a normal subgroup of G. Let l be the soluble length of M. We know that M^{l-1} is a nontrivial abelian normal subgroup of G. Thus, $M^{l-1} \subseteq K^*$, and hence for every $x \in M^{l-1}$ we have $x^{2^\alpha} = RN_{C_D(K)/K}(x) = 1$, which contradicts the fact that M is of odd order. Therefore, M is trivial and so $H' \simeq Q_8$. One may easily show that other cases are also true by similar arguments and this proves the case (iv).

We are now prepared to prove the following.

Theorem 1. *Let D be an F-central division algebra of index q^r, q a prime. If D^* contains an irreducible soluble subgroup, then D is a crossed product.*

Proof. We may consider the following two cases:

Case 1. $Char F = p > 0$. By Lemma 3, we know that there is an irreducible soluble subgroup G and abelian normal subgroup K^* of G such that $K = K^* \cup \{0\}$ is a subfield of D and G/K^* as well as H' is finite, where $H = C_G(K^*)$. Since $Char F = p > 0$, by a result of [4, p.215], we conclude that H' is cyclic. Now, by Lemma 3, G/K^* is a q-group and hence it is nilpotent. Thus, G is an irreducible abelian-by-nilpotent subgroup of D^*. Now, by Theorem C, we conclude that D is a nilpotent crossed product, which completes the proof of this case.

Case 2. $Char F = 0$. We keep to the notations of the case 1. If H' is abelian, then as in the above case we obtain the result. So, we may assume that H' is nonabelian. By Lemma 3, we know that H^{t-2} is a finite q-group. If q is odd, then, by a result of [9, p.45], we conclude that H^{t-2} is cyclic, which contradicts the fact that H^{t-2} is nonabelian. So, we may assume that $q = 2$. We now proceed by induction on r. If $r = 1$, then it is clear that D is cyclic. Assume that the result holds for all $n < r$. Now, by a result of [9, p.45] again, we conclude that H^{t-2} is cyclic or a (generalized) quaternion. Since H^{t-2} is nonabelian we conclude that H^{t-2} is a (generalized) quaternion. As in the proof of Lemma 3, one may easily show that $H^{t-2} \simeq Q_8$. Therefore, H^{t-2} is normal in G. Set $D_1 = F[H^{t-2}]$. It is clear that $i(D_1) = 2$ and $Z(D_1) = F$ and D_1 is a crossed product. Now, by the Double Centralizer Theorem, we have $D \simeq D_1 \otimes_F C_D(D_1)$. Since G normalizes D_1 we see that for any $g \in G$ we may define a natural homomorphism $f_g : D_1 \to D_1$, given by the rule $f_g(x) = gxg^{-1}$ for any $x \in D_1$. Hence, by Skolem-Noether Theorem there is an element $a_g \in D_1^*$ such that $f_g = f_{a_g}$. If $u, v \in D_1$ satisfy $f_u = f_v$, then for any $x \in D_1$ we have $uxu^{-1} = vxv^{-1}$. Therefore, $u^{-1}v \in Z(D_1) = F$, which shows that u, v are equal modulo F^*, i.e., $F^*u = F^*v$. Now, for any $x \in D_1$ we have $gxg^{-1} = a_gxa_g^{-1}$, and hence $b_g := a_g^{-1}g \in C_D(D_1)$. The fact that b_g commutes with a_g implies that a_g, g, and b_g pairwise commute. Set $A = \cup_{g\in G} F^* a_g$ and $B = \cup_{g\in G} F^* b_g$. We claim that A, B are groups. To see this, it is enough to show that for any $g, h \in G$ we have $F^*a_{g^{-1}} = F^*a_g^{-1}, F^*a_h a_g = F^*a_{hg}, F^*b_{g^{-1}} = F^*b_g^{-1}, F^*b_h b_g = F^*b_{hg}$. For any $x \in D_1, f_{a_{g^{-1}}}(x) = f_{g^{-1}}(x) = g^{-1}xg = (a_g b_g)^{-1}x(a_g b_g) = a_g^{-1}xa_g = f_{a_g^{-1}}(x)$. Therefore, $F^*a_{g^{-1}} = F^*a_g^{-1}$. Also, we have $f_{a_{hg}}(x) = f_{hg}(x)$. Hence $f_{a_{hg}}(x) = hgxg^{-1}h^{-1} = ha_g x a_g^{-1}h^{-1} = a_h a_g x a_g^{-1}a_h^{-1} = (a_h a_g)x(a_h a_g)^{-1} = f_{a_h a_g}(x)$. Therefore, $F^*a_h a_g = F^*a_{hg}$ which shows that A is a group. Next, considering the fact that $a_g \in D_1$ and $b_h \in C_D(D_1)$ we obtain $b_h b_g = b_h a_g^{-1}g = a_g^{-1}b_h g = a_g^{-1}a_h^{-1}hg = (a_h a_g)^{-1}hg$. Thus, since A is a group we conclude that $F^*b_h b_g = F^*(a_h a_g)^{-1}hg = F^*a_{hg}^{-1}hg = F^*b_{hg}, F^*b_g^{-1} = F^*a_g g^{-1} = F^*a_{g^{-1}}^{-1}g^{-1} = F^*b_{g^{-1}}$. Therefore, B is also a group. We claim that B is soluble that is normalized by G. To see this, consider the epimorphism $\theta : G \to B/F^*$ given by $\theta(g) = F^*b_g$ for all $g \in G$. Hence B/F^* as a homomorphic image of a soluble group is soluble, and so is B. Set $D_2 = C_D(D_1)$. If we show that $D_2 = F[B]$, then by induction D_2 is a crossed product. To prove this, put $D_3 = F[B]$. Now, for all $g \in G$ we have $g = a_g b_g = (a_g \otimes 1)(1 \otimes b_g) = a_g \otimes b_g$. Therefore, we conclude that $G \subset D_1 \otimes D_3$ and hence $F[G] = D = D_1 \otimes D_3 = D_1 \otimes D_2$. Finally, one may easily see that $[D_3 : F] = [D_2 : F]$, and so $D_3 \subseteq D_2$, i.e., $D_3 = D_2$ and so the result follows.

Let D be an F-central division algebra of degree p^r, p a prime. Using the above result one may conclude that if D^* contains an irreducible finite subgroup G, then D is a crossed product. To see this, by a result of [9, p.51, Thm 2.1.11], we know that either G is soluble or $G \simeq SL_2(Z_5)$. If the first case happens, then the result follows from Theorem 1. If the second case occurs, then as in the course of the proof of Theorem 2.1.11 of [9, p.51], we have $[\mathbb{Q}(G) : \mathbb{Q}] \leq 8$. Since $\mathbb{Q} \subseteq F$ we clearly have $[F[G] : F] \leq 8$ and hence $[D : F] = 4$ because G is irreducible. Therefore, D is cyclic and so the result also follows for this case. Later on we shall present a different proof of this fact which may be of some interest. Now, combining Lemma 1 and Theorem 1, we are able to obtain one of our main results in the following form.

Corollary 1. *Let D be an F-central division algebra of index p^r, p a prime. Then, D is a crossed product if and only if D^* contains an irreducible soluble subgroup.*

4 Irreducible abelian-by-finite subgroups

This section turns to the case where the multiplicative group D^* contains an irreducible abelian-by-finite subgroup. Let D be an F-central division algebra of index p^r, p a prime. It is proved that except when $CharF = 0$ and $p = 2, r > 1$, D is a crossed product if and only if D^* contains an irreducible abelian-by-finite subgroup. Furthermore, the conclusion also holds for the excluded case provided that D^* contains no finite subgroup isomorphic to $SL_2(Z_5)$. Using the above result, and the Tits Alternative which asserts that a finitely generated linear group either contains a non-cyclic free subgroup or it is soluble-by-finite [11], we are able to show that D is a crossed product if and only if D^* contains an irreducible subgroup satisfying a group identity. Furthermore, the conclusion also holds for the above excluded case provided that D^* contains no finite subgroup isomorphic $SL_2(Z_5)$. To prove our results, we shall need the following lemma.

Lemma 4. *Given a field F of characteristic zero, let D be an F-central division algebra of index $2^r, r > 1$. Assume that D^* contains an irreducible abelian-by-finite subgroup. If D is a non-crossed product, then D^* contains a copy of the finite group $SL_2(Z_5)$.*

PROOF. Suppose that G is an irreducible abelian-by-finite subgroup of D^* and A is a maximal abelian normal subgroup of G such that G/A is finite. Set $K = F(A)$. It is clear that $G \subseteq N_D{}^*(K^*)$, and hence $G_1 = GK^*$ is an irreducible subgroup of D^* so that G_1/K^* is finite. One may easily show that K^* is a maximal abelian normal subgroup of G_1. Put $H = C_{G_1}(K^*)$. By maximality of K^*, we have $Z(H) = K^*$. Now, we know that $H/Z(H)$ is finite, and so by Theorem of [8, p.443, Thm. 15.1.13], the derived group H' is a finite group. We claim that H' is nonabelian. For if H' is abelian, then H is soluble. Now, by Lemma A, we have $G_1/H \simeq Gal(K/F)$ and K/F is a Galois extension. Thus, G_1/H is a 2-group and hence G_1 is soluble. We note that G_1 is an irreducible soluble subgroup of D^*. By Theorem 1, we conclude that D is a crossed product which is a contradiction. Thus, H' is nonabelian as claimed. Therefore, by a result of [9, p.51], this implies that either H' is a soluble group or $H' \simeq SL_2(Z_5)$. If the first case occurs, then H is soluble and hence as above

G is soluble. Therefore, by Theorem 1, we conclude that D is a crossed product which is a contradiction. So, we have $H' \simeq SL_2(Z_5)$, and the result follows.

Theorem 2. *Let D be an F-central division algebra of index q^r, q a prime. If D^* contains an irreducible abelian-by-finite subgroup, then, except for the case $CharF = 0$ and $q = 2, r > 1$, D is a crossed product. Furthermore, the conclusion also holds for the above excluded case provided that D^* contains no finite subgroup isomorphic to $SL_2(Z_5)$.*

Proof. We consider the following three cases:
Case 1. $CharF = p > 0$. Suppose that G is an irreducible abelian-by-finite subgroup of D^* and A is a maximal abelian normal subgroup of G such that G/A is finite. Set $K = F(A)$. It is clear that $G \subseteq N_D{}^*(K^*)$, and hence $G_1 = GK^*$ is an irreducible subgroup of D^* so that G_1/K^* is finite. One may easily show that K^* is a maximal abelian normal subgroup of G_1. Put $H = C_{G_1}(K^*)$. By maximality of K^*, we have $Z(H) = K^*$. Now, we know that $H/Z(H)$ is finite, and so by Theorem of [8, p.443], the derived group H' is a finite group. Thus, by a result of [4, 4, Cor. 13.3], we conclude that H' is cyclic. Therefore, H is a soluble group. Now, by Lemma A, we have $G_1/H \simeq Gal(K/F)$ and K/F is a Galois extension. Thus, G_1/H is q-group and hence G_1 is soluble. We note that G_1 is an irreducible soluble subgroup of D^*. By Theorem 1, we conclude that D is a crossed product, which completes the proof of this case.
Case 2. $CharF = 0$. If $q = 2$ and $r = 1$, then it is clear that D is cyclic. So, we may assume that q is odd. Keeping to the notations of the above case, we know that $H/Z(H)$ is finite as well as the derived group H'. Therefore, by a result of [9, p.51], we know that either H' is a soluble group or $H' \simeq SL_2(Z_5)$. In the first case H is soluble and as in the above case we have that G_1 is also a soluble subgroup of D^*. Thus, by Theorem 1, we conclude that D is a crossed product. We claim that the second case leads to a contradiction. So, we may assume that $H' \simeq SL_2(Z_5)$. In the course of the proof of Theorem 2.1.11 of [9, p.51], that the only finite insoluble subgroup of a division ring is $SL_2(Z_5)$ we obtain $[\mathbb{Q}(H') : \mathbb{Q}] \leq 8$. Since $\mathbb{Q} \subseteq K$ we conclude that $[K[H'] : K] \leq 8$. On the other hand, we have $K \subseteq Z(K[H'])$. Set $D_1 = K[H']$. Now, we know that D_1 is a division algebra

with $[D_1 : Z(D_1)] \leq 8$. Therefore, $[D_1 : Z(D_1)] = 4$ and hence 2 divides q^r, which contradicts our assumption that q is odd.
Case 3. Assume that $Char F = 0, p = 2$, and $r > 1$. If D is not a crossed product, then, by Lemma 4, we conclude that D^* contains a copy of the finite group $SL_2(Z_5)$, which is a contradiction. This completes the proof of the theorem.

Combining Lemma 1 and Theorem 2, we obtain the following.

Corollary 2. *Let D be an F-central division algebra of index p^r, p a prime. Then, except when $Char F = 0$ and $p = 2, r > 1$, D is a crossed product if and only if D^* contains an irreducible abelian-by-finite subgroup. Furthermore, the conclusion also holds for the above excluded case provided that D^* contains no finite subgroup isomorphic to $SL_2(Z_5)$.*

Using the above result, and the Tits Alternative which asserts that a finitely generated linear group either contains a non-cyclic free subgroup or it is soluble-by-finite [11], we are able to prove the following criterion.

Corollary 3. *Let D be an F-central division algebra of index p^r, p a prime. Then, except when $Char F = 0$ and $p = 2, r > 1$, D is a crossed product if and only if D^* contains an irreducible subgroup satisfying a group identity. Furthermore, the conclusion also holds for the above excluded case provided that D^* contains no finite subgroup isomorphic to $SL_2(Z_5)$.*

PROOF. The "only if " part is clear by Lemma 1. Assume that G is an irreducible subgroup of D^* satisfying a group identity. Since $[D : F] < \infty$ we may view G as a linear group. Let G_1 be a subgroup of G generated by the elements of a basis of D over F. Thus, by Tits Alternative, we know that G_1 is soluble-by-finite, i.e., there is a soluble normal subgroup N of G_1 such that G_1/N is finite. Now, by Lemma 3 of [5], N is abelian-by-finite. Thus, G_1 is abelian-by-finite. Therefore, by Theorem 2, D is crossed product.

Now, one may apply the above results to prove the following criterion for D to be cyclic. This is one of the main results of [2].

Corollary 4. *Let D be an F-central division algebra of prime degree p. Then D is cyclic if and only if D^* contains a nonabelian subgroup satisfying a group identity.*

PROOF. The "only if" part is clear by Lemma 1. If $p = 2$, then D is cyclic. Let p be an odd prime. Now, by Corollary 3, one can easily show that D is cyclic. □

Let D be an F-central division algebra of finite index $i(D) = n$ and G be an irreducible subgroup of D^*. Assume that A is a maximal abelian normal subgroup of G. We conclude this section with some remarks concerning the relation between the cardinal of G/A and the dimension of D/F.

Remark 1. Let D be a finite dimensional F-central division algebra. If G is an irreducible subgroup of D^* with maximal abelian normal subgroup A such that G/A is nilpotent, then $|G/A| = i(D)$. To see this, set $G_1 = K^*G$, where $K = F[A]$. It is easily seen that G_1 is irreducible with maximal abelian normal subgroup K^* such that $G_1/K^* \simeq G/A$ and so G_1/K^* is nilpotent. As in the proof of Theorem 3.4 of [3], one may easily check that K/F is Galois and K is a maximal subfield of D. Therefore, we have $C_{G_1}(K^*) = K^*$. Now, by Lemma B, we have $G_1/K^* \simeq Gal(K/F)$, i.e., $|G_1/K^*| = |G/A| = [K : F] = i(D)$.

Remark 2. Let D be an F-central division algebra of index p^r, p a prime. Assume that G is an irreducible subgroup of D^* with maximal abelian subgroup A such that G/A is finite. Then, except when $Char F = 0$ and $p = 2, r > 1$, we have $|G/A| = i(D)$. Furthermore, the conclusion also holds for the excluded case provided that D^* contains no finite subgroup isomorphic to $SL_2(Z_5)$. To prove this, we may use Theorem 1, Theorem 2, and the Remark 1 to obtain the result.

5 Irreducible finite subgroups

Let D be an F-central division algebra of degree p^r, p a prime. This section studies the structure of D under the condition that D^* has an irreducible finite subgroup. Using Amitsur's classification of finite multiplicative subgroups of a division ring, it is proved that if D^* contains an irreducible finite subgroup, then D is a crossed product.

Theorem 3. *Let D be an F-central division algebra of index q^r, q a prime. If D^* contains an irreducible finite subgroup G, then D is a crossed product.*

Proof. We first observe that $Char F = 0$. Since otherwise G is cyclic and since G is irreducible we obtain $D = F$ which is a contradiction. If q is odd, then the result follows from Corollary 3. So we may assume that $q = 2$. By a result of [9, p.51], we know that either G is soluble or $G \simeq SL_2(Z_5)$. If the second case occurs, then as in the course of the proof of Theorem 2.1.11 of [9, p.51], that the only finite insoluble subgroup of a division ring is $SL_2(Z_5)$, we may obtain $[\mathbb{Q}(G) : \mathbb{Q}] \leq 8$. Since $\mathbb{Q} \subseteq F$ we clearly have $[F[G] : F] \leq 8$ and hence $[D : F] = 4$ because G is irreducible. Therefore, D is cyclic and so the result follows for this case. It remains to consider the case where G is soluble and $q = 2$. By Lemma 3 of [5], we know that G is abelian-by-finite, i.e., there is an abelian normal subgroup A in G of finite index. Take A maximal in G, and set $K = F(A)$. One may easily show that $G \subseteq N_{D^*}(A)$ and that $G_1 = K^*G$ is an irreducible soluble subgroup of D^* with maximal abelian normal subgroup K^*. Set $H = C_G(A)$, $H_1 = C_{G_1}(K^*)$. It is clearly seen that $H_1 = HK^*$. Since elements of K^* and H pairwise commute we conclude that $H_1' = H'$. Now, by Lemma B, K/F is Galois with $G_1/H_1 \cong Gal(K/F)$. Therefore, G_1/H_1 is a 2-group and hence it is nilpotent. Now, one may easily show that $G \cap H_1 = H$ and $G_1 = GK^* = GH_1$. Thus, we have $G_1/H_1 \cong G/H$ and hence G/H is a 2-group. If H_1' is abelian, then as in the proof of Lemma 3, one may easily show that H_1/K^* is a 2-group. Now, since $A = H \cap K^*$ and $H_1 = HK^*$ we conclude that H/A is a 2-group. This means that G/A is also a 2-group and hence G is abelian-by-nilpotent. Therefore, by Theorem C, we conclude that D is crossed product. Thus, we may assume that $H_1' = H'$ is nonabelian. Let $l(H) = t$ be the derived length of H. As in the proof of Lemma 3, one may easily show that H^{t-2} is a nonabelian 2-group and it is isomorphic to the quaternion group Q_8. This means that H contains a normal subgroup isomorphic to Q_8. Now, assume that $T = O_2(H)$ is a maximal normal 2-subgroup of H. As in Lemma 3, it is easily seen that $O_2(H) \simeq Q_8$. Now, by a result of [9, p.54], we have either $H \simeq Q_8 \times M$, where M is a group of odd order, or $H \simeq SL_2(Z_3) \times M$, where M is a group of order m coprime to 6, or H is isomorphic to the binary octahedral group. We deal with these cases separately as follows:

Case 1. $H \simeq Q_8 \times M$, where M is a group of odd order. We claim that M is normal in G. Since H is normal in G for each $g \in G$ and $m \in M$ we have $gmg^{-1} = (q, m_1) \in H$. Comparing the orders of both sides of the last relation, one may easily conclude that $q = 1$ and so the claim is established. Now, we show that M is abelian. Otherwise, M' is nontrivial. If l is the soluble length of M, then $l \geq 2$. Thus, $M^{l-1} \subseteq M'$ is a nontrivial abelian subgroup. This implies that AM^{l-1} is an abelian normal subgroup of G and hence by the choice of A we obtain $M^{l-1} \subseteq A$. By Lemma B, we know that $F[H_1] = C_D(K)$. Since $M \subseteq H \subseteq H_1$ we obtain $M' \subseteq C_D(K)'$. Take an element $x \in M^{l-1} \subseteq A \subseteq K^*$. We have $1 = RN_{C_D(K)/K}(x) = x^{2^s}$, where $i(C_D(K)) = 2^s$. This shows that the order of x is a power of 2 which contradicts the fact that M has odd order. Hence M' must be trivial and so M is abelian. It is clear that $H/M \simeq Q_8$ and $G_1/H_1 \simeq G/H$ is a 2-group. Since M is normal in G we conclude that G/M is also a 2-group. This says that G is abelian-by-nilpotent and hence, by Theorem C, D is a crossed product.

Case 2. $H \simeq SL_2(Z_3) \times M$. Since the order of M is prime to 6 and $|SL_2(Z_3)| = 24$, as in the case 1, we conclude that M is an abelian normal subgroup of G. Now, M as an abelian normal subgroup of D^* is cyclic. Set $M =< m >$ such that for each natural number s with $(s, 6) = 1$ we have $m^s = 1$. Since $SL_2(Z_3) \subseteq G$ we have $2||G|$ and hence there exists $g \in G$ such that $g^2 = 1$, i.e., $-1 \in G$.

If $m \in F^*$, then $m \in Z(G)$. Therefore, $1, m, \cdots, m^{s-1}, -1, -m, \cdots, -m^{s-1}$ are distinct elements of $Z(G)$ for if $m^i = -m^j$ with $0 \leq i, j \leq s-1$, then raising to the power of s we obtain $1 = -1$ which is a contradiction to the fact that $CharF = 0$. Thus, $|Z(G)| > 2s$. Now, G as an irreducible subgroup of D^* contains a basis $g_1, g_2, \cdots, g_t$ with $t = 2^{2r}$. Since $g_1, g_2, \cdots, g_t$ are linearly independent over F we conclude that $g_1Z(G), g_2Z(G), \cdots, g_tZ(G)$ are distinct elements of $G/Z(G)$ and hence $|G/Z(G)| \geq t$. Therefore, we have $|G| \geq 2^{2r} \times 2s$. On the other hand, we have $|M| = s$ and so $|H| = 2^3 \times 3 \times s$ and also $G/H \simeq Gal(K/F)$, where K/F is Galois. If $[K : F] = 2^r$, then K is a maximal subfield of D and hence D is crossed product. So, we may assume that $[K : F] \leq 2^{r-1}$. In this case we obtain $|G| \leq 2^3 \times 3 \times s \times 2^{r-1}$. Therefore, $2^{2r+1} \times s \leq 2^{r+2} \times 3 \times s$ which implies that $2^{r-1} \leq 3$, i.e., $r = 1$ or $r = 2$. If $r = 1$, then it is clear that D is cyclic. If $r = 2$, then, by a result of [7, p. 183], D is a crossed product.

If $m \notin F^*$, then MA is an abelian normal subgroup of G. By maximality of A, we conclude that $M \subseteq A \subseteq K^*$. Since m is not in F we obtain $|Gal(K/F)| = 2^u$ with $u \geq 1$. Since $Z(H)$ is an abelian normal subgroup of G, by maximality of A , we have $Z(H) = A$. Therefore, $A =< -1 > \times M$ and hence $|A| = 2s$. Since Q_8 is normal in G let $O_2(G) = Q_{2^l}$. It is clearly seen that $(Q_{2^l})^2 =< x^2 >$, where $Q_{2^l} =< x, y | x^{2^{l-1}} = y^4 = 1, yxy^{-1} = x^{-1} >$. Now, one may easily show that $N =< x^2 >$ is normal in G. Since the orders of M and N are coprime we have $M \cap N = 1$. Therefore, each element of M commutes with each element of N, i.e., MN is abelian. Since $-1 \in N$ we obtain $A \subseteq MN$. But this contradicts the choice of A unless $< x^2 >=< -1 >$, i.e., $x^4 = 1$ and $l = 3$. Thus, $O_2(G) = Q_8$. Now, by a result of [9, p.54] again we have three subcases to consider as follows:

Subcase 1. $G \simeq Q_8 \times M_1$, where the order of M_1 is odd. If $|M_1| = 2n + 1$, then $|G| = 2^3 \times (2n + 1)$. Now, we have $|H| = 2^3 \times 3 \times s$, where s is odd, and $|G/H| = |Gal(K/F)| = 2^u$ with $K \neq F$. Therefore, $(2n + 1) = 3s \times 2^u$ which is not possible.

Subcase 2. $G \simeq SL_2(Z_3) \times M_1$, where the order of M_1 is prime to 6. Since the order of M_1 is odd, as in the Subcase 1, we obtain a contradiction.

Subcase 3. G is isomorphic to the binary octahedral group of 48 elements. Then, $|G| = 2^4 \times 3$. Since $-1 \in Z(G)$ we obtain $|Z(G)| \geq 2$. As before, because G is irreducible we have $|G/Z(G)| \geq 2^{2r}$. Therefore, $2^{2r+1} \leq 2^4 \times 3$. This means that either $r = 1$ or $r = 2$, and as above we conclude that D is a crossed product.

Case 3. H is isomorphic to the binary octahedral group of 48 elements. Then, $|H| = 2^4 \times 3$. As in the Subcase 3, we conclude that $|G| \geq 2^{2r+1}$. In addition, as in the previous cases, we have $|G/H| < 2^{r-1}$, and hence $|G| \leq 2^{r-1} \times 2^4 \times 3$, i.e., $2^{2r+1} \leq 2^{r+3} \times 3$. This implies that either $r = 1$ or $r = 2$ or $r = 3$. For the cases $r = 1$ or $r = 2$, as before, we conclude that D is crossed product. Assume that $r = 3$. If D is not a crossed product, then, by Lemma 3, D^* contains a copy of Q_8. It is clear that $[F[Q_8] : F] = 4$. Set $B = F[Q_8]$. Then, by Centralizer Theorem, we have $D \simeq B \otimes C_D(B)$. Since $i(C_D(B)) = 4$, by a result of [7, p. 183], $C_D(B)$ is a crossed product. Therefore, D which is a tensor product of crossed products is a crossed product division algebra. This completes the proof of the theorem.

The authors thank the Research Council of Sharif University of Technology for support.

References

[1] P. K. Draxl, *Skew fields*, LMS Lecture Notes Series 81, (1983).

[2] R.Ebrahimian, D.Kiani and M.Mahdavi-Hezavehi, *Irreducible Subgroups of $GL_1(D)$ Satisfying Group Identities*, Comm. Alg., to appear.

[3] R.Ebrahimian, D.Kiani and M.Mahdavi-Hezavehi, *Supersoluble crossed product criterion for division algebras* , Israel Journal of Mathematics, to appear.

[4] T. Y. Lam, *A first course in noncommutative rings* , GTM, No. 131, Springer-Verlag, 1991.

[5] M. Mahdavi-Hezavehi, *Free subgroups in maximal subgroups of $GL_1(D)$*, J. Alg. 241 (2001) 720-730.

[6] M. Mahdavi-Hezavehi and J. P. Tignol, *Cyclicity conditions for division algebras of prime degree*, Proc. Amer. Math. Soc., 131 (2003), 3673-3676.

[7] L. Rowen, Ring theory, Volume II, Academic Press, INC, (1988).

[8] W. R. Scott, *Group theory, Dover*, New York 1987.

[9] M. Shirvani and B. A. F. Wehrfritz, *Skew linear group*, LMS Lecture Note Series, No. 118, 1986.

[10] D. A. Suprunenko, *On solvable subgroups of multiplicative groups of a field*, English Transl., Amer. Math. Soc. Transl., (2)46(1965), p. 153-161.

[11] A. E. Zalesskii, Linear groups, in “Algebra IV,” part II (A. I. Kostrikin, I. R. Shafarevich, Eds.), Encyclopedia of Mathematics and Science, Springer-Verlag, Berlin/New York, 1993.