JOURNAL OF ALGEBRA 163, 795–805 (1994)

# Projective Schur Division Algebras Are Abelian Crossed Products*

ELI ALJADEFF

*Department of Mathematics, Technion, Haifa, Israel*

AND

JACK SONN

*Department of Mathematics, Technion, Haifa, Israel*

*Communicated by Alexander Lubotzky*

Received January 27, 1992

Let $k$ be a field. A projective Schur Algebra over $k$ is a finite-dimensional $k$-central simple algebra which is a homomorphic image of a twisted group algebra $k^\alpha G$ with $G$ a finite group and $\alpha \in H^2(G, k^*)$. The main result of this paper is that every projective Schur division algebra is an abelian crossed product $(K/k, f)$, where $K$ is a radical extension of $k$. 

## 1. INTRODUCTION AND STATEMENT OF RESULTS

Let $k$ be any field. A finite-dimensional $k$-central simple algebra $B$ is called a *Schur algebra* if it is the homomorphic image of a group algebra $kG$ for some finite group $G$. The classes in the Brauer group $Br(k)$ containing Schur algebras form a subgroup $S(k)$ of $Br(k)$ called the *Schur group* of $k$ [Y]. The Schur group has been generalized by Lorenz and Opolka [LO] by replacing group algebras $kG$ by *twisted* group algebras $k^\alpha G$ where $\alpha \in H^2(G, k^*)$, $k^* =$ the multiplicative group of $k$, and $k^\alpha G$ is the $k$-algebra with basis $\{u_\sigma \mid \sigma \in G\}$ and multiplication rule given by

$$u_\sigma u_\tau = a(\sigma, \tau) u_{\sigma\tau},$$

* This research was supported in part by the Fund for the Promotion of Research at the Technion. A significant part of the research in this paper was carried out during a visit to the University of Antwerp in October 1991. The authors are grateful to Professor F. Van Oystaeyen and the University of Antwerp for their hospitality.



0021-8693/94 $6.00

where $a(\sigma, \tau) \in \alpha$. Thus a projective Schur algebra over $k$ is a finite-dimensional $k$-central simple algebra $B$ which is a homomorphic image of a twisted group algebra $k^\alpha G$ for some finite group $G$ and some $\alpha \in H^2(G, k^*)$. (If char $k = 0$ then a $k$-central simple algebra $B$ is a homomorphic image of a twisted group algebra $k^\alpha G$ if and only if $B$ is a direct summand of $k^\alpha G$).

The classes in $Br(k)$ containing projective Schur algebras form a subgroup $PS(k)$, known as the *projective Schur group* of $k$. Lorenz and Opolka [LO] proved that $PS(k) = Br(k)$ if $k$ is a number field and it has been observed by Van Oystaeyen [NVO] that the Merkuriev–Suslin Theorem [M] implies that if $k$ is a field containing the $n^{\text{th}}$ roots of unity, then $PS_n(k) = Br_n(k)$, where the subscript $n$ denotes the subgroup of elements of order dividing $n$. It has been asked [NVO] if $PS(k) = Br(k)$ for all fields.

In this paper we will not deal with $PS(k)$, but with the structure of *projective Schur division algebras*, that is, division algebras that are projective Schur algebras. The analogous question for Schur algebras was answered by Amitsur [A], in the process of determining the finite subgroups of division algebras, since the subalgebra of a division algebra $D$ generated over $k$ by a finite subgroup of $D^*$ is a Schur division algebra. A noncommutative Schur division algebra $D$ is always a symbol algebra $(a, \omega)_n$ (see below), where $k(a^{1/n})$ is a cyclotomic extension of $k$, and $\omega$ is a root of unity. More generally, a Schur algebra $B$ is always similar to a *cyclotomic* algebra, see [Y], i.e., a crossed product $(K/k, \alpha)$ with $\alpha \in H^2(G(K/k), K^*)$, where $K = k(\zeta)$ is a cyclotomic extension of $k$, and $\alpha$ contains a cocycle $a(\sigma, \tau)$ with values in a finite group $W$ of roots of unity in $K$. Any cyclotomic algebra $B = (K/k, \alpha)$ is a Schur algebra in a natural way since the group $E$ defined by the group extension $\alpha$

$$1 \to W \to E \to G(K/k) \to 1$$

is a finite subgroup of $B$ spanning $B$ over $k$, so $B$ is a homomorphic image of the group ring $kE$. Similarly there is a natural way of constructing a *projective* Schur algebra. First note that a $k$-central simple algebra $B$ is a projective Schur algebra if and only if there is a multiplicative subgroup $\Gamma$ of $B$ containing $k^*$ such that $\Gamma/k^*$ is finite, and $\Gamma$ spans $B$ over $k$ as a $k$-vector space, i.e., $B = k(\Gamma)$. Indeed, the group $\Gamma$ is the group extension

$$1 \to k^* \to \Gamma \to G \to 1$$

defined by $\alpha$ if $B$ is a homomorphic image of $k^\alpha G$, and conversely, if $B = k(\Gamma)$ then $B$ is a homomorphic image of $k^\alpha G$, where $G = \Gamma/k^*$ and $\alpha$ corresponds to the group extension

$$1 \to k^* \to \Gamma \to G \to 1.$$

Thus, to construct a projective Schur algebra over $k$, start with any finite *radical* Galois extension $K/k$. $K/k$ is a radical extension if and only if $K=k(A)$ where $A$ is a subgroup of $K^*$ such that $A/k^*$ is a torsion group. Thus, if $K/k$ is a finite radical extension, then $A/k^*$ is finite. If $K/k$ is also Galois, then we may assume $A$ is $G$-invariant, $G=G(K/k)$. Now, take any $\alpha \in H^2(G, A)$ and its image $\alpha' \in H^2(G, K^*)$. The crossed product $(K/k, \alpha')$ contains the group $\Gamma$ defined as the group extension of $A$ and $G$ determined by $\alpha$:

$$1 \to A \to \Gamma \to G \to 1.$$

Since $K=k(\Gamma)$, $\Gamma/k^*$ is finite and $(K/k, \alpha')$ is central simple, $(K/k, \alpha')$ is a projective Schur algebra. We will call such an algebra a *radical* algebra.

The simplest example of such an algebra is a *symbol* algebra $(a, b)_n$. If $k$ contains a primitive $n^{\text{th}}$ root of unity $\zeta$, and $a, b \in k^*$ then $(a, b)_n$ is generated over $k$ by $u, v$ satisfying $u^n=a$, $v^n=b$, $vu=\zeta uv$. We see $(a, b)_n$ is a projective Schur algebra by taking $A=\langle u \rangle$ and $\Gamma=\langle u, v \rangle$. Similarly, a tensor product of symbols is a projective Schur algebra, which proves the observation quoted above, that $PS_n(k)=Br_n(k)$ when $k$ contains the $n^{\text{th}}$ roots of unity, since $Br_n(k)$ is generated by symbols, by Merkuriev–Suslin.

On the other hand, not every cyclic algebra is a projective Schur algebra, as we will see later. Let us now state the main result of this paper. A radical algebra $(k(A)/k, \alpha')$ is called an *abelian* radical algebra if $k(A)/k$ is an abelian extension.

THEOREM 1. *Let $k$ be any field, $D$ a projective Schur division algebra with center $k$. Then $D$ is an abelian radical algebra over $k$. In particular $D$ is an (abelian) crossed product $(K/k, \alpha')$.*

Before turning to the proofs, we make two remarks which are relevant to the structure theory of projective Schur algebras and projective Schur groups.

*Remark* 1. Let $M_r(D)$ denote the $r \times r$ matrix ring over a division ring $D$. Then $M_r(D)$ may be a projective Schur algebra without $D$ being one.

*Remark* 2. Let $D$ be a $k$-division algebra of degree $n=p_1^{e_1} \cdots p_s^{e_s}$, $P_i$ prime, $i=1, ..., s$, $D \cong D_1 \otimes_k \cdots \otimes_k D_s$ where $D_i$ is a $k$-division algebra of degree $p_i^{e_i}$, $i=1, ..., s$ [R, p. 256]. Then $D$ may be a projective Schur algebra without all the $D_i$ being so.

To prove these two remarks, we first show that Remark 2 implies Remark 1.

Suppose $M_r(D)$ projective Schur implies $D$ projective Schur. We show then that if $D=D_1 \otimes \cdots \otimes D_s$ is a projective Schur $k$-division algebra of degree $n = p_1^{e_1} \cdots p_s^{e_s}$, with degree $D_i = p_i^{e_i}$, $1 \leqslant i \leqslant s$, then all the $D_i$ are projective Schur as well. In the Brauer group of $k$, $[D] = [D_1] \cdots [D_s]$ where $\exp[D_i] = p^{d_i}$, $d_i \leqslant e_i$. It follows that each $[D_i]$ is a power of $[D]$. If $D$ is a projective Schur algebra, then $[D] \in PS(k)$, and therefore $[D_i] \in PS(k)$ too. This implies that $M_r(D_i)$ is a projective Schur algebra for some $r$, hence $D_i$ is a projective Schur algebra.

To prove Remark 2, we will give an example of a cyclic projective Schur division algebra $D$ with primary decomposition $D \simeq D_1 \otimes \cdots \otimes D_s$ and not all the $D_i$ are projective Schur. To this end, we consider the very special case of projective Schur division algebras of prime degree $p$. The following proposition is really a special case of Theorem 1, but we will give a separate and more elementary proof of it here.

PROPOSITION 1. *Let $D$ be a projective Schur division algebra of prime degree $p$ over $k$. Then either $D$ is a cyclic algebra $(k(\zeta)/k, \sigma, a)$ with $\zeta$ a root of unity, or $D$ is a symbol algebra $(a, b)_p$ where $k$ contains the $p^{\text{th}}$ roots of unity.*

*Proof.* Let $D = k(\Gamma)$, $\Gamma \leqslant D^*$, $\Gamma/k^*$ finite. Let $x \in \Gamma \backslash k$, such that the order of $x \bmod k^*$ is a prime $q$. Setting $a = x^q$, the polynomial $X^q - a$ is either irreducible over $k$ or has a root in $k$ (see [VdW], p. 180]). If $X^q - a$ has a root $b$ in $k$, then the other roots are of the form $\zeta^i b$, with $\zeta$ a primitive $q^{\text{th}}$ root of unity. Thus $k(x) = k(\zeta)$ is a cyclotomic extension of $k$. Suppose now that for *all* $x \in \Gamma$ of prime order modulo $k^*$, $X^q - a$ is irreducible over $k$, where $q =$ order of $x$ modulo $k^*$. Then since $[k(x):k] = q$, $q = p$, so $\Gamma/k^*$ is a finite $p$-group. Let $z \in \Gamma \backslash k^*$ be central and of order $p$ modulo $k^*$. Since $z$ is not central in $\Gamma$ $(Z(\Gamma) \subset Z(D) = k)$ we have for some $x \in \Gamma$, $(x^{-1}zx)^p = a = (\zeta z)^p = \zeta^p z^p = \zeta^p a$. Thus $\zeta^p = 1$ so $\zeta$ is a primitive $p^{\text{th}}$ root of unity. Clearly $D = k(z, x)$ so $x^p \in Z(D) = k$. Thus $D$ is a symbol algebra $(a, b)_p$. ∎

*Note.* The proposition shows that the only way for a division algebra of prime degree $p$ to be a projective Schur algebra is in one of two obvious ways. Not every cyclic algebra of prime degree $p$ is of this type. For example, let $K$ be any cyclic extension of prime degree $p \neq 2$ of $\mathbb{Q}$. Then, the extension $K/\mathbb{Q}$ is neither cyclotomic nor Kummer. On the other hand, it is known that every cyclic extension of $\mathbb{Q}$ can be embedded as a maximal subfield of a $\mathbb{Q}$-division algebra $D$ [Sch], which, by Proposition 1, is not a projective Schur algebra if $[K:\mathbb{Q}] = p$.

Consider now the following example. Let $q$ be a prime such that $q - 1$ is divisible by some odd prime $p$ but not by $p^2$, e.g., $q = 7$, $p = 3$. Let $L$ be the field of $q^{\text{th}}$ roots of unity. Let $D$ be a $\mathbb{Q}$-division algebra containing $L$ as a maximal subfield. Then $D$ is a projective Schur algebra. Now

$D = D_2 \otimes D_3$ with $D_2, D_3$ of exponent ($=$index) 2, 3, respectively. By Proposition 1, $D_3$ is not a projective Schur algebra. This proves Remark 2 and hence Remark 1.

## 2. Proof of Theorem 1

*Remark* 3. A finite abelian subgroup $A$ of the multiplicative group of a $k$-division algebra $D$ is necessarily cyclic, since it is contained in the field $k(A)$.

LEMMA 1. *Let $D$ be a projective Schur division algebra over $k$, $\Gamma$ a spanning group over $k$, with $\Gamma/k^*$ finite. Then*

(a) *The commutator subgroup $\Gamma'$ of $\Gamma$ is finite,*

(b) *Let $A$ be a finite abelian normal subgroup of $\Gamma$. Then $\Gamma'$ centralizes $A$.*

(c) *If $A$ is a maximal abelian subgroup of $\Gamma'$ and is also a normal subgroup of $\Gamma$, then $\Gamma' = A$ is abelian.*

*Proof.* Part (a) follows from the fact that the center $Z(\Gamma)$ of $\Gamma$ is of finite index in $\Gamma$, by [Sc, p. 443]. To prove (b), observe that $A$ is cyclic, so $\mathrm{Aut}(A)$ is abelian. It follows that $\Gamma$ acts on $A$ through an abelian quotient, so $\Gamma'$ acts trivially on $A$. Part (c) follows from (b) by taking an element $x \in \Gamma' \backslash A$ (if $\Gamma' \neq A$) and observing that $\langle x, A \rangle$ is abelian. ▮

MAIN LEMMA. *Let $D$ be a projective Schur division algebra over its center $k$. Then there is a spanning group $\Gamma$ of $D$ over $k$, $\Gamma/k^*$ finite, such that either:*

(a) *$\Gamma'$ is cyclic; or*

(b) *$\Gamma$ contains a normal subgroup $H$ isomorphic to the quaternion group $Q_8$ of order* 8.

*Proof.* If $\operatorname{char} k = p > 0$, then $\mathbb{F}_p(\Gamma')$ is a finite division algebra, hence a field, so $\Gamma'$ is (finite) abelian hence cyclic. We may therefore assume $\operatorname{char} k = 0$. We now apply Amitsur's classification [A, p. 382] of finite multiplicative subgroups of division algebras to enumerate the possibilities for $\Gamma$.

*Case* 1. $\Gamma'$ is a metacyclic group $G_{m,r}$ generated by $X$, $Y$ with relations $X^m = 1$, $Y^n = X^t$, $YXY^{-1} = X^r$ where $n$ is the order of $r \bmod m$ (i.e., $\Gamma'/\langle X \rangle$ acts faithfully on $\langle X \rangle$). $\Gamma'' = G'_{m,r} = \langle X^s \rangle$, $\langle Z(\Gamma') \rangle = \langle X^t \rangle$, where

$s=(r-1,m)=m/t$. In addition the integers $n, m, s, t$ satisfy one of two possibilities:

(1.1) $n, s$, are odd and $(n,t)=(s,t)=1$

(1.2) $n=2n'$, $s=2s'$, $m=2^{\alpha}m'$, $\alpha\geqslant 2$, where $n', s', m'$ are odd; $(n,t)=(s,t)=2$, $r\equiv -1 \bmod(2^{\alpha})$.

Assume (1.1). The subgroups $Z(\Gamma')=\langle X^t\rangle$ and $\Gamma''=\langle X^s\rangle$ are characteristic in $\Gamma'$; therefore, since $(s,t)=1$, the cyclic subgroup $\langle X\rangle$ generated by $X$ is also characteristic in $\Gamma'$ hence normal in $\Gamma$. By Lemma 1, $\Gamma'$ centralizes $\langle X\rangle$, hence $\Gamma'$ is abelian and therefore cyclic. Assume now (1.2). By a similar argument, the cyclic subgroup generated by $\langle X^2\rangle$ is contained in $Z(\Gamma')$. Since $t\equiv 0 \pmod 2$, $Z(\Gamma')=\langle X^t\rangle=\langle X^2\rangle$. Finally, using $t\mid m$ and $r\equiv -1 \pmod{2^{\alpha}}$ we conclude $t=2$, $s=m/2=(r-1,m)$, $n=2$. This shows that the group $\Gamma'$ in this case is generated by elements $X$ and $Y$ with the relations $X^m=1$, $Y^2=X^2$, $YXY^{-1}=X^r$, $r\equiv -1 \pmod{2^{\alpha}}$, $n=t=2$, $m=2^{\alpha}m'$, $\alpha\geqslant 2$, $m'=\text{odd}$, $\text{ord}(\Gamma')=2m$. Now for $p\neq 2$ the $p$-Sylow subgroups in $\langle X\rangle$ are also $p$-Sylow subgroups in $\Gamma'$. They are characteristic in $\langle X\rangle$ so normal and therefore also characteristic in $\Gamma'$. This shows that the subgroup $\langle X^{2^{\alpha}}\rangle$ of order $m'$ is characteristic in $\Gamma'$. Consider the central extension

$$1\to\langle X^{2^{\alpha}}\rangle\to\Gamma'\to\Gamma'/\langle X^{2^{\alpha}}\rangle\to 1.$$

Since $\gcd(\text{ord}(\langle X^{2^{\alpha}}\rangle), \text{ord}(\Gamma'/\langle X^{2^{\alpha}}\rangle))=1$, the extension splits, so there is a subgroup $H$ in $\Gamma'$ isomorphic to $\Gamma'/\langle X^{2^{\alpha}}\rangle$. Clearly $H$ is of order $2^{\alpha+1}$ and characteristic in $\Gamma$. We claim that $H$ is isomorphic to $Q_8$, the quaternion group of order 8. Indeed, it is generated by elements $\bar{X}=x$ and $\bar{Y}=y$ with $x^{2^{\alpha}}=1$, $x^2=y^2$, $yxy^{-1}=x^{-1}$. Thus, $y=x^2yx^{-2}=x(xyx^{-1})x^{-1}=x^4y$, i.e., $x^4=1$. This completes the proof of the main lemma for the case $\Gamma'\cong G_{m,r}$.

*Case* 2. $\Gamma'\cong\hat{A}_4$, the binary tetrahedral group of order 24.

*Case* 3. $\Gamma\cong\hat{S}_4$, the binary octahedral group of order 48.

Both groups contain characteristic subgroups isomorphic to $Q_8$ (quaternions of order 8).

*Case* 4. $\Gamma'\cong\hat{A}_5$, the binary icosahedral group of order 120. We have an exact sequence

$$1\to\{\pm 1\}\to\hat{A}_5\to A_5\to 1.$$

$\hat{A}_5$ contains the binary tetrahedral group $\hat{A}_4$ as a subgroup of index 5. Now $\text{Aut}(A_5)=S_5$ (see, e.g., [HB, p. 391]). Since $\hat{A}_5$ is contained in a double cover $\hat{S}_5$ of $S_5$ (there are two in fact; see [So]), we have $S_5 \subseteq \mathrm{Aut}(\hat{A}_5)$. Since every automorphism of $\hat{A}_5$ induces an automorphism of $A_5$ we have $\mathrm{Aut}(\hat{A}_5) \cong \mathrm{Aut}(A_5) \simeq S_5$.

*Claim.* The conjugates of $\hat{A}_4$ in $\hat{A}_5$ form a characteristic class of conjugate subgroups in $\hat{A}_5$, i.e., the set of conjugates of $\hat{A}_4$ in $\hat{A}_5$ is invariant under $\mathrm{Aut}\,\hat{A}_5$. This is equivalent to the assertion that the conjugates of $A_4$ in $A_5$ are a characteristic class in $A_5$. The number of conjugates of $A_4$ in $S_5$ is $[S_5 : N_{S_5}(A_4)] = [S_5 : S_4] = 5$, proving the claim since $S_5 = \mathrm{Aut}\,A_5$.

We may now apply the Frattini argument [Ro, p. 194] to obtain

$$\Gamma = N_\Gamma(\hat{A}_4)\hat{A}_5.$$

Now consider the subalgebra $\mathbb{Q}(\Gamma')$. Clearly it is a division algebra and using [A, Lemma 14], we have

$$\mathbb{Q}(\Gamma') \simeq U_2 \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{5}), \qquad U_2 = \text{rational quaternions}.$$

Thus $Z(\mathbb{Q}(\Gamma')) = \mathbb{Q}(\sqrt{5})$.

*Case* 4.1. $\sqrt{5} \in k$. Then, extending the scalars to $k$, we get $k(\Gamma') =$ quaternions over $k$. Now the normalizer $N_\Gamma(\hat{A}_4)$ contains $\hat{A}_4$ so it also contains $Q_8$. Since $k(Q_8)$ is a quaternion algebra over $k$ contained in $k(\Gamma')$, we have $k(Q_8) = k(\Gamma')$. It follows that $k(\Gamma') \subset k(N_\Gamma(\hat{A}_4))$ and since $\Gamma = N_\Gamma(\hat{A}_4)\Gamma'$ we have $k(\Gamma) = k(N_\Gamma(\hat{A}_4))$. We replace $\Gamma$ by $\Gamma_0 = N_\Gamma(\hat{A}_4)$. Since $Q_8$ is characteristic in $\hat{A}_4$ it is normal in $\Gamma_0$ as desired.

*Case* 4.2. $\sqrt{5} \notin k$. Then the center of $k(\Gamma')$ is $k(\sqrt{5})$. The group $\Gamma$ acts on $k(\Gamma')$ so it acts on $k(\sqrt{5})$. It fixes only elements of $k$ so it sends $\sqrt{5}$ to $-\sqrt{5}$ ($\sqrt{5}$ is not in the center of $k(\Gamma)$. Let $\tilde{\Gamma} = \langle \sqrt{5}, \Gamma \rangle \subset D^*$. Then $\tilde{\Gamma}/k^*$ is finite. The quaternion group $Q_8$ is contained in $\hat{A}_4$, which is contained in $\Gamma'$. The algebra $k(\Gamma')$ is the quaternion algebra over $k(\sqrt{5})$. Also the algebra $k(\sqrt{5})(Q_8)$ is a quaternion algebra over $k(\sqrt{5})$ and is contained in $k(\Gamma')$. Therefore $k(\sqrt{5})(Q_8) = k(\Gamma')$. Since $N_\Gamma(\hat{A}_4) \subset N_{\tilde{\Gamma}}(\hat{A}_4)$ and both $\hat{A}_4$ (so $Q_8$) and $\sqrt{5}$ normalize $\hat{A}_4$ we see that $k(\Gamma') \subset k(N_{\tilde{\Gamma}}(\hat{A}_4))$. Write $\Gamma_0 = N_{\tilde{\Gamma}}(\hat{A}_4)$. We have $k(\Gamma) = k(N_\Gamma(\hat{A}_4)\Gamma') \subseteq k(N_{\tilde{\Gamma}}(\hat{A}_4)\Gamma') \subseteq k(N_{\tilde{\Gamma}}(\hat{A}_4))\,k(\Gamma') \subseteq k(N_{\tilde{\Gamma}}(\hat{A}_4)) = k(\Gamma_0)$. Thus $k(\Gamma) = k(\Gamma_0)$. Now $Q_8$ is characteristic in $\hat{A}_4$ so normal in $\Gamma_0$. So, if we replace $\Gamma$ by $\Gamma_0$, we get the main lemma for this case, and this in fact completes the proof of the main lemma.

We now consider the two situations of the main lemma. In the first, we prove that the conclusion of Theorem 1 holds, and in the second, $D$

decomposes into a tensor product of a projective Schur division algebra and a quaternion algebra, which yields a proof of Theorem 1 by induction.

PROPOSITION A. *Let $D = k(\Gamma)$ be a projective Schur k-division algebra. If $\Gamma'$ is abelian (i.e., cyclic) then Theorem* 1 *is true*: *$D$ is an abelian radical algebra.*

*Proof.* Let $A$ be a maximal abelian subgroup of $\Gamma$, containing $\Gamma'$. Let $K = k(A)$. Since $A \supset \Gamma'$, it is normal in $\Gamma$ and so $\Gamma$ acts on $K = k(A)$. Let $P$ be the kernel of this action. By maximality of $A$ we have $P = A$. Write $G = \Gamma/A$. Finally, by a dimension argument we show that the field extension $K/k$ is Galois and that $K$ is a maximal subfield of $D$. Let $[D:k] = n^2$. Then $[K:k] = m \leqslant n$ and $|G| = s \leqslant m$ (since $G \subseteq \mathrm{Aut}(K/k)$). Recall that $\Gamma$ spans $D$ over $k$ so any section of $G$ into $\Gamma$ spans $D$ over $K$ (as a vector space). Then

$$n^2 = \dim_k D = \dim_k K \cdot \dim_K D \leqslant m \cdot s \leqslant n^2.$$

Therefore, $m = s = n$ and $K$ is a maximal subfield in $D$, Galois over $k$. This completes the proof. ∎

PROPOSITION B. *Let $D$ be a projective Schur division algebra over $k$, $D = k(\Gamma)$, $\Gamma$ a spanning group $\subseteq D^*$, $\Gamma/k^*$ finite. Suppose $\Gamma$ contains a normal subgroup $H$ isomorphic to the quaternion group $Q_8$ of order* 8. *Then $D = D_1 \otimes_k D_2$ with $D_1 =$ the ordinary quaternion algebra over $k$, and $D_2$ is a projective Schur division algebra.*

*Proof.* First note that the subalgebra $D_1 = k(H)$ of $D$ is isomorphic to the ordinary quaternions over $k$, since $D_1$ is a noncommutative division algebra and the center of $H$ must be $\{\pm 1\} \subseteq k$. The action of $\Gamma$ on $H$ by conjugation induces a homomorphism

$$\Gamma \to \mathrm{Aut}(H) \cong S_4.$$

Let $\hat{S}_4$ denote the binary octahedral group. We have an exact sequence

$$1 \to \{\pm 1\} \to \hat{S}_4 \to S_4 \to 1.$$

There is a known embedding of $\hat{S}_4$ into the multiplicative group of the ordinary quaternions $\mathbb{H}_{\mathbb{Q}(\sqrt{2})}$ over $\mathbb{Q}(\sqrt{2})$ extending the embedding of the binary tetrahedral group $\hat{A}_4$ into $\mathbb{H}_{\mathbb{Q}}$ [V, p. 17]. We have $\hat{A}_4 \cong E_{24} \subset \mathbb{H}_{\mathbb{Q}}$ where

$$E_{24} = \{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}$$

and

$$\hat{S}_4 = E_{48} = E_{24} \cup \left\{ (\pm\alpha \pm \beta)/\sqrt{2} \colon \{\alpha, \beta\} \subset \text{2-element subsets of } \{1, i, j, k\} \right\}.$$

Consider the subgroup $N$ of $\mathbb{H}_{\mathbb{Q}}^*$ generated by $E_{24}$ and

$$S = \left\{ \pm\alpha \pm \beta \mid \{\alpha, \beta\} \subset \text{2-element subsets of } \{1, i, j, k\} \right\}.$$

Then $N$ is a subgroup of $\mathbb{H}_{\mathbb{Q}}^*$ containing $E_{24}$ with $N\langle\sqrt{2}\rangle = E_{48}\langle\sqrt{2}\rangle$. Now $Nk^*/k^*$ is finite. Indeed, $[Nk^* : k^*] = [N : N \cap k^*] \leqslant [N : N \cap \langle 2\rangle] = [N : \langle 2\rangle] = [N\langle\sqrt{2}\rangle : \langle\sqrt{2}\rangle] = [E_{48}\langle\sqrt{2}\rangle : \langle\sqrt{2}\rangle] = |E_{48}| = 48$ since $E_{48} \cap \langle\sqrt{2}\rangle = \{1\}$. Since the action of $E_{48}$ on $H$ maps $E_{48}$ onto $\mathrm{Aut}(H) \cong S_4$, the action of $N$ on $H$ maps $N$ onto $\mathrm{Aut}(H) = S_4$ too. We claim $\Gamma$ normalizes $N$. Indeed, since $N \subset k(H)$ and $N \supset H$ it is clear that $C_{D^*}(H) = C_{D^*}(N)$ where $C_{D^*}$ denotes the centralizer in $D^*$. Let $\gamma \in \Gamma$. There exists $v \in N$ such that $\gamma v^{-1} \in C_{D^*}(H)$. Hence $\gamma = (\gamma v^{-1})v$ normalizes $N$, proving the claim. Now set $\hat{\Gamma} = \Gamma N$. Then $\hat{\Gamma}/k^*$ is finite since $|\hat{\Gamma}/k^*| = |\Gamma N/k^*| \leqslant |\Gamma/k^*|\,|Nk^*/k^*| < \infty$. The group $\hat{\Gamma}$ contains $\Gamma$ so that $k(\hat{\Gamma}) = D$. Consider now the action of $\hat{\Gamma}$ on $H$. The induced homomorphism $\hat{\Gamma} \to \mathrm{Aut}(H) \simeq S_4$ is onto since $\hat{\Gamma} \supset N$. Let $\hat{\Gamma}_0$ be its kernel. Given $\gamma \in \hat{\Gamma}$, there is $v \in N$ such that $\gamma v^{-1} \in \hat{\Gamma}_0$. Hence $\hat{\Gamma} = \hat{\Gamma}_0 N$. It follows that

$$D = k(\hat{\Gamma}) = k(\hat{\Gamma}_0)\, k(N) = k(\hat{\Gamma}_0)\, k(H).$$

Now $k(\hat{\Gamma}_0)$ and $k(H)$ centralize each other, so $k(\hat{\Gamma}_0) \subset C_D(k(H))$, which we denote by $D_2$. Since $D = D_1 \otimes_k D_2 = D_1 \otimes_k k(\hat{\Gamma}_0)$ we have $D_2 = k(\hat{\Gamma}_0)$ and the proof is complete. ∎

By successive applications of Proposition B with the observation that the tensor product of radical algebras is again a radical algebra, we have reduced the proof of Theorem 1 to Proposition A, hence Theorem 1 is proved. (In fact, at most one application of Proposition B is reguired.)

Another consequence of Propositions A and B is that we can choose $\Gamma$ with abelian commutator. We record this in

COROLLARY 1. *Let $D$ be a projective Schur division algebra. Then there exists a spanning group $\Gamma$ (finite modulo $k^*$) such that $\Gamma'$ is abelian.*

*Proof.* This is clear if we remember that $Q_8' = \{\pm 1\}$ is abelian. ∎

Another immediate consequence of Propositions A and B is:

COROLLARY 2. *Let $D$ be a projective Schur division algebra with center $k$. Let $\Gamma$ be a spanning group, finite modulo $k^*$. If* $\dim_k D = \text{odd}$, *then $\Gamma'$ is abelian (therefore cyclic).*

*Proof.* Clearly in this case $D$ contains no subalgebra isomorphic to the quaternion algebra over $k$. ▮

*Remark* 4. *If* char $k = p \neq 0$ *and index* $D = p^m$ *then the radical extension* $K/k$ *in Theorem* 1 *is a cyclotomic extension.*

The proof of Remark 4 follows from the following

PROPOSITION C. *Let* $k$ *be a field of characteristic* $p \neq 0$ *and let* $K = k(\mathrm{A})$ *be a radical Galois extension of degree* $p^m > 1$. *Then* $K$ *is a cyclotomic extension of* $k$.

*Proof.* We first prove the following special case: $|A/k^*| =$ a prime $q$. Let $\alpha \in A \backslash k$, so $\alpha^q = a \in k^*$. Suppose the polynomial $X^q - a$ is irreducible over $k$. Then $[k(\alpha) : k] = q$, so $q = p$, $k(\alpha)/k$ is inseparable, a contradiction. Then by [VdW, p. 180], $X^q - \mathrm{a}$ has a root $b \in k$, so $\alpha/b = \zeta$ is a $q^{\text{th}}$ root of unity and $k(\alpha) = k(\zeta)$, which proves the proposition in this special case.

We now prove the proposition in the general case by induction on $m$. If $m = 1$, then take any $\alpha \in \mathrm{A} \backslash k$ of prime order mod $k^*$. Then $k(\alpha) \neq k$, so $k(\alpha) = k(A)$ and we are in the special case above. Now assume $m > 1$, and again take any $\alpha \in A \backslash k$ of prime order mod $k^*$. Then $[k(\alpha) : k] > 1$ and by the special case, $k(\alpha)/k$ is cyclotomic. Since $[k(A) : k(\alpha)] = p^r < p^m$, we have by induction $k(A)/k(\alpha)$ is cyclotomic. It follows that $k(A)/k$ is cyclotomic.

*Note added in proof.* During the research on this paper, the first author had a useful discussion with M. Shirvani, who has since informed the author that he has obtained some partial results along the lines of the present paper.

## REFERENCES

[A] S. AMITSUR, Finite subgroups of division rings, *Trans. Amer. Math. Soc.* **80** (1955), 361–386.

[HB] B. HUPPERT AND N. BLACKBURN, "Finite Groups, III," Springer, New York, 1982.

[LO] F. LORENZ AND H. OPOLKA, Einfache Algebren und projektive Darstellungen über Zahlkörpern, *Math. Z.* **162** (1978), 175–182.

[M] A. S. MERKURIEV, $K_2$ of fields and the Brauer group, *in* "Proceedings Boulder Conf. on $K$-theory, 1983."

[R] I. REINER, "Maximal Orders," Academic Press, Orlando, FL, 1975.

[Ro] J. ROTMAN, "An Introduction to the Theory of Groups," Allyn & Bacon, New York, 1984.

[Sch] M. SCHACHER, Subfields of division rings, I, *J. Algebra* **9** (1968), 451–477.

[Sc] L. SCOTT, "Group Theory," Prentice–Hall, New Jersey, 1964.

[So] J. SONN, Double covers of $S_5$ and Frobenius groups as Galois groups over number fields, *J. Algebra* **114** (1988), 401–410.

[VdW] B. L. VAN DER WAERDEN, "Algebra," Vol. I, Ungar, New York, 1970.

[V] M.-F. VIGNERAS, Arithmétique des Algèbres de Quaternions, *in* "Lecture Notes in Mathematics," Vol. 800, Springer-Verlag, New York/Berlin, 1980.

[NVO] P. NELIS AND F. VAN OYSTAEYEN, The projective Schur subgroup of the Brauer group and root groups of finite groups, *J. Algebra* **137** (1991), 501–518.

[Y] T. YAMADA, The Schur subgroup of the Brauer group, *in* "Lecture Notes in Mathematics," Vol. 397, Springer-Verlag, New York/Berlin, 1970.