Exponent Reduction for Radical Abelian Algebras

Eli Aljadeff and Jack Sonn

Department of Mathematics, Technion, 32000 Haifa, Israel
E-mail: aljadeff@math.technion.ac.il, sonn@math.technion.ac.il

Communicated by A. Lubotzky

Received September 10, 1998

Let $k$ be a field. A radical abelian algebra over $k$ is a crossed product $(K/k, \alpha)$, where $K = k(T)$ is a radical abelian extension of $k$, $T$ is a subgroup of $K^*$ which is finite modulo $k^*$, and $\alpha \in H^2(G, K^*)$ is represented by a cocycle with values in $T$. The main result is that if $A$ is a radical abelian algebra over $k$, and $m = \exp(A \otimes k(\mu))$, where $\mu$ denotes the group of all roots of unity, then $k$ contains the $m$th roots of unity. Applications are given to projective Schur division algebras and projective Schur algebras of nilpotent type. © 2000 Academic Press

1. INTRODUCTION AND SUMMARY OF RESULTS

Let $k$ be any field and $Br(k)$ be its Brauer group. The projective Schur group of $k$ is the subgroup of $Br(k)$ which consists of all classes that may be represented by projective Schur algebras. A $k$-central simple algebra $A$ is a projective Schur algebra if it is spanned as a $k$-vector space by a subgroup $\Gamma'$ of the units of $A$ which is finite modulo its center (note that we may assume that the center of $\Gamma'$ is $k^*$). Equivalently, a $k$-central simple algebra $A$ is projective Schur if it is the homomorphic image of a twisted group algebra $k^*S$ for some finite group $S$ and some $\alpha \in H^3(S, k^*)$. The projective Schur group $PS(k)$ can be viewed as the projective analogue of the Schur group $S(k)$ which arises from group algebras (or representations of finite groups) over $k$. Recall that a Schur algebra over $k$ is a $k$-central simple algebra which is the homomorphic image of a group algebra $kS$ for some finite group $S$ (or equivalently, $k$ central simple algebras that are

---

1 This research was supported by the Fund for the Promotion of Research at the Technion and the Technion VPR Fund.
spanned by a finite subgroup of the units). The Schur group $S(k)$ is the subgroup generated by (and in fact consisting of) Brauer classes that may be represented by Schur algebras over $k$. Clearly $S(k) \leq PS(k) \leq Br(k)$. One of the main features of the projective Schur group is that it contains all the (classes of) symbol algebras. Indeed every symbol algebra over $k$ can be written as a twisted group algebra (and in particular as a homomorphic image). Invoking the Merkurev–Suslin theorem [8], it follows that if the field $k$ contains all roots of unity, then $PS(k) = Br(k)$. Moreover, it is a result of [6] that if $k$ is a number field, then again $PS(k) = Br(k)$. In general, the projective Schur group is not equal to the full Brauer group.

In [3] it is shown that $PS(k)$ is contained in the relative Brauer group $H^2(\text{Gal}(L/k), L^*)$ where $L$ is the compositum of the maximal cyclotomic extension of $k$ and the maximal Kummer extension of $k$ (in particular $L/k$ is abelian). Furthermore it is shown there that, for $k = F(x)$, a rational function field in one variable over a number field $F$, there are Brauer classes that are not split by $L$. It is not known whether $PS(k) = H^2(\text{Gal}(L/k), L^*)$.

There is a natural way to construct projective Schur algebras, which yields the so-called radical algebras. Recall that a finite extension $K/k$ is radical if it is obtained by taking roots of elements of $k^*$. More precisely $K/k$ is radical if the elements in $K$ which are finite modulo $k$ span $K$ over $k$. Clearly, when $K/k$ is Galois with group $G$, this is equivalent to saying that $K^*$ contains a spanning $G$-invariant subgroup $N$, which is finite modulo $k^*$. A $k$-central simple algebra $A$ is called radical if it is isomorphic to a crossed product $(K/k, G, \alpha)$, where $K/k$ is a radical extension and the class $\alpha \in H^2(G, K^*)$ may be represented by a 2-cocycle whose values in $K^*$ are of finite order modulo $k^*$. We point out that to any radical algebra we can associate a group extension $1 \to N \to \Gamma \to G \to 1$ where $K = k(N)$ and $N$ is finite modulo $k^*$. Clearly, $|\Gamma/k^*| < \infty$ and $A = k(\Gamma)$, which shows that $A$ is a projective Schur algebra over $k$. If one restricts (in the construction of radical algebras) to cyclotomic extensions (rather than radical) and to cocycles with values that are roots of unity (rather than values of finite order modulo $k^*$) one obtains “cyclotomic algebras over $k$.” It is easy to see that such algebras are spanned over $k$ by a finite subgroup of the units of $A$. In particular $A$ is a Schur algebra. An important theorem of Brauer and Witt [10, Chapter 3] states that every class in $S(k)$ may be represented by a cyclotomic algebra. In [2] it has been conjectured that the projective analogue of the Brauer–Witt theorem holds, namely, that every class in $PS(k)$ may be represented by a radical algebra. Combining this with the fact that every projective Schur algebra is split by the compositum of Kummer and cyclotomic extensions of $k$ and in particular by a radical abelian extension (i.e., the Galois group is abelian) we conjecture that every projective Schur algebra is Brauer equivalent to a radical abelian algebra.

In [1] the conjecture is proved for projective Schur algebras which are
division algebras. In [4] it is proved (although only stated for radical algebras) that the conjecture holds for projective Schur algebras \( k(\Gamma) \) over \( k \) of nilpotent type (a projective Schur algebra \( k(\Gamma) \) over \( k \) is of nilpotent type if \( \Gamma \) or equivalently \( \Gamma/k^* \), can be chosen to be a nilpotent group).

The purpose of this article is to show that radical abelian algebras satisfy a rather restrictive condition. Let \( \mu \) denote the group of all roots of unity (in an algebraic closure of \( k \)).

1.1. **Main Theorem.** Let \( A = (K/k, G, \alpha) \) be a radical abelian algebra. Then the exponent of \( A \otimes_k k(\mu) \) divides the number of roots of unity in \( k \), or more precisely, \( k \) contains a primitive root of unity of order exp\((A \otimes_k k(\mu))\).

1.2. **Corollary.** Let \( D/k \) be a division algebra which is spanned over \( k \) by a subgroup of the units which is finite modulo the center. Then the exponent of \( D \otimes_k k(\mu) \) divides the number of roots of unity in \( k \).

1.3. **Corollary.** Let \( P \text{Nil}(k) \) denote the subgroup of \( Br(k) \) which consists of classes that may be represented by projective Schur algebras of nilpotent type. Then for any \( \alpha \in P \text{Nil}(k) \), res\(_{k(\mu)/k}(\alpha) \) has order dividing the number of roots of unity in \( k \).

For elements in \( P \text{Nil}(k) \) more is true. Let \( \mu_{p^n} \) denote the group of all roots of unity of \( p \)-power order.

1.4. **Theorem.** Let \( \alpha \in P \text{Nil}(k) \) have order \( n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} \). Then the order of res\(_{k(\mu_{p_1^{n_1} \cdots p_r^{n_r}})/k}(\alpha) \) divides the number of roots of unity in \( k \).

(Here \( k(\mu_{p_1^{n_1} \cdots p_r^{n_r}}) \) denotes the cyclotomic extension of \( k \) obtained by joining all \( p_i \)-power roots of unity, \( i = 1, \ldots, r \).)

**Remark.** We can use Theorem 1.4 to sharpen our knowledge about the inclusion \( P \text{Nil}(k)_p \subset PS(k)_p \subset Br(k)_p \). In general, \( P \text{Nil}(k)_p \) is a proper subgroup of \( Br(k)_p \); in fact, if \( k \) does not contain the \( p \)-th roots of unity, then \( P \text{Nil}(k)_p = 0 \) [6, 4]. On the other hand, if the field \( k \) contains the \( p \)-th roots of unity, \( P \text{Nil}(p)_p \) can be quite large; for example if \( k \) is a number field containing the \( p \)-th roots of unity, then \( P \text{Nil}(p)_p = PS(p)_p = Br(k)_p \) [6]. We use Theorem 1.4 to show that \( P \text{Nil}(k)_p \) may be a proper subgroup of \( PS(k)_p \) even if \( k \) contains the \( p \)-th roots of unity. We point out that examples of fields \( k \) (which may or may not contain the \( p \)-th roots of unity) for which \( PS(k)_p \) is a proper subgroup of \( Br(k)_p \) are given in [3].

**Example.** Consider the (constant) Galois extension \( K \) of \( \mathbb{Q}(x) \) obtained by adjoining a fifth root of unity. The Galois group is cyclic of order 4 with generator, say \( \sigma \). Let \( D = (K/\mathbb{Q}(x), \sigma, x) \) be the cyclic algebra of index 4 defined by the equation \( u_4^4 = x \). \( D \) has exponent 4 and is therefore a division algebra. To see this, it suffices to verify that \( x \) has order 4 modulo the norm group \( N_{K/\mathbb{Q}(x)}(K^*) \), and for this we may pass to the formal power
series field \( \mathbb{Q}(x) \). Here we see that the extension obtained by adjoining a fifth root of unity is an unramified extension, so every norm has valuation divisible by 4; hence \( x \) has order 4 mod norms. The same argument shows that \( D \otimes_{\mathbb{Q}(x)} \mathbb{Q}(x, \mu_2^n) \) also has exponent 4. We observe next that \( D \) is a radical abelian algebra. Theorem 1.4 now implies \([D] \not\in P \text{Nil}(\mathbb{Q}(x))_2\).

As pointed out above it is not known whether \( PS(k) \) is a proper subgroup of the relative Brauer group \( \text{Br}(L/k) = H^2(\text{Gal}(L/k), L^*) \) where \( L \) is the compositum of the maximal cyclotomic extension of \( k \) and the maximal Kummer extension of \( k \). We construct a variant of the previous example by replacing the cyclotomic extension \( \mathbb{Q}(\mu_5)/\mathbb{Q} \) by a regular (over \( F \)) extension \( K = F(t, x) \) which is cyclic of degree four, and \( F \) is a field of characteristic zero (see, for example, [7, p. 224]). Here \( x, t \) are algebraically independent over \( F \). Let \( D \) be the cyclic algebra \( (K(x)/F(t, x), \sigma, x) \). The same argument as above shows that \( D \) is of exponent four and therefore a division algebra. Clearly the exponent of \( D \) is not reduced by tensoring up to any cyclotomic extension. On the other hand, \( D \) is split by a \( \mathbb{Z}_2 \times \mathbb{Z}_2 \) Kummer extension, namely, the (maximal) subfield generated over \( F(t, x) \) by \( \sqrt{x} \) and the quadratic subfield of \( K \). Suppose that \( F = \mathbb{Q} \) or any field of characteristic zero not containing the fourth roots of unity. Theorem 1 above and [1, Theorem 1] then imply that \( D \) is not isomorphic to a projective Schur algebra and also not Brauer equivalent to a radical abelian algebra. Note that a positive answer to our conjecture above would imply \([D] \not\in PS(F(x, t)) \) and hence \( PS(k) \not\in \text{Br}(L/k) \), where \( k = F(x, t) \).

2. PRELIMINARIES

Recall that a projective Schur algebra \( k(\Gamma) \) over \( k \) is reduced if the subalgebra \( k(H) \) is simple for any subgroup \( H \) of \( \Gamma \) containing the commutator subgroup \( \Gamma' \).

Let \( A = (K/k, G, \alpha) \) be a radical abelian algebra with associated group extension \( 1 \to N \to \Gamma \to G \to 1 \). Since the group \( G \) is abelian the commutator \( \Gamma' \leq N \) is also abelian.

2.1. LEMMA. Let \( k(\Gamma) \) be a projective Schur algebra over \( k \) with \( \Gamma' \) abelian. Then it is equivalent to a reduced projective Schur algebra \( k(\Sigma) \) with \( \Sigma' \) abelian.

Proof. In [2] it is shown that every projective Schur algebra \( k(\Gamma) \) over \( k \) (not necessarily with abelian commutator) is equivalent to a reduced algebra \( k(\Sigma) \) where \( \Sigma \) is obtained from \( \Gamma \) by a finite sequence of taking subgroups and quotient groups. \( \blacksquare \)
In the main proof we will need a kind of converse to the statement preceding the lemma (see [4, Prop. 3.1]).

2.2. PROPOSITION. Let \( k(\Gamma) \) be a reduced projective Schur algebra with \( \Gamma' \) abelian. Then \( k(\Gamma) \) is a radical abelian algebra; that is, there is a group extension \( 1 \to N \to \Gamma \to G \to 1 \) with \( G \) abelian and \( k(\Gamma) = (k(N)/k, G, \alpha) \). Furthermore, if \( N_0 \) is an abelian subgroup of \( \Gamma' \) containing \( \Gamma'' \), then we can choose an associated group extension \( 1 \to N \to \Gamma \to G \to 1 \) with \( N \supseteq N_0 \).

Proof. It is sufficient to prove the second statement. Let \( N \) be a maximal abelian subgroup of \( \Gamma' \) containing \( \Gamma'' \). Clearly, \( N \) is normal and \( \Gamma/N \) is abelian. Denote the latter by \( G \). The reducedness of \( k(\Gamma') \) implies \( k(\Gamma') \) is simple and therefore a field extension of \( k \). Observe that conjugation with elements of \( \Gamma \) induces an action of \( G \) on \( k(\Gamma') \). Furthermore the action is faithful since \( N \) is maximal abelian in \( \Gamma' \). Finally we note that \( G \cong \text{Gal}(k(N)/k) \) since the center of \( k(\Gamma') \) is \( k \).

3. PROOFS

From the previous section we see that in order to prove Theorem 1.1 it is sufficient (and in fact equivalent) to show that for any reduced projective Schur algebra \( k(\Gamma) \) with \( \Gamma' \) abelian, \( \text{ord}(k(\Gamma') \otimes_k k(\mu)) \) divides the number of roots of unity in \( k \). The subalgebra \( k(\Gamma') \) is commutative (since \( \Gamma' \) is an abelian group); moreover it is a field extension of \( k \) since \( k(\Gamma') \) is reduced. Recall that \( \Gamma' \) is center by finite and hence, by a well known theorem due to Schur, the commutator \( \Gamma'' \) is finite. This implies of course that \( k(\Gamma') \) is a cyclotomic extension of \( k \). Consider the family \( \Omega \) of abelian subgroups in \( \Gamma' \) that contain \( k(\Gamma') \). Let \( \Omega_c = \{ T \in \Omega : k(T)/k \text{ cyclotomic} \} \). Observe that \( \Omega_c \) is not empty since it contains \( k^* \Gamma' \). Let \( H_0 \in \Omega_c \) be a maximal element (with respect to inclusion) and let \( H \) be the centralizer of \( k(H_0) \) in \( \Gamma' \).

3.1. LEMMA. (a) \( \Gamma/H \cong \text{Gal}(k(H_0)/k) \),
(b) \( k(\Gamma) \otimes_k k(H_0) \sim k(H) \),
(c) \( \text{ord}(k(\Gamma) \otimes_k k(\mu)) \) divides \( \text{ord}(k(\Gamma') \otimes_k k(H_0)) \).

Proof. (a) Since \( H \) is the centralizer of \( k(H_0) \) in \( \Gamma' \), the group \( \Gamma/H \) acts faithfully on \( k(H_0) \). To show it is equal to the full Galois group over \( k \) let \( x \in k(H_0)^G \). Clearly \( x \) commutes with all elements in \( \Gamma' \) and since \( \Gamma' \) spans the algebra \( k(\Gamma) \) over \( k \), \( x \) must be in the center \( k \).
(b) By Proposition 2.2 there is a maximal abelian subgroup $N$ in $\Gamma$ with $k^\Gamma H \leq H_0 \leq N \leq H \leq \Gamma$ and such that $k(\Gamma) = (k(N)/k, \Gamma/N, \alpha)$ where $\alpha: 1 \to N \to \Gamma \to \Gamma/N \to 1$. Furthermore $k(H) = (k(N)/k(H_0), H/N, \text{res}(\alpha))$ where $\text{res}(\alpha)$ denotes the restriction of $\alpha$ to $H/N$. It follows that the map $\text{res}: H^2(\Gamma/N, k(N)^*) \to H^2(H/N; k(N)^*)$ maps $k(\Gamma)$ to $k(H)$ so that (b) holds.

(c) Clear, since $k(H_0) \subseteq k(\mu)$.

From Lemma 3.1 we see that it is sufficient to show that the order of $[k(H)]$ in $\text{Br}(k(H_0))$ divides the number of roots of unity in $k$. To this end observe that the group $H$ spans $k(H)$ over the center $k(H_0)$ (since it does over $k$) and moreover $H$ is abelian modulo $k(H_0)^*$. $(H_0 \supseteq \Gamma^0)$ This says that that $[k(H)]$ is contained in $P\text{Ab}(k(H_0))$. Recall that $P\text{Ab}(F)$ is the subgroup of $PS(F)$ consisting of elements that may be represented by projective Schur algebras $F(\Lambda)$ where $\Lambda/F^*$ is (finite) abelian. In the next lemma we bound the order of $F(\Lambda)$ in $\text{Br}(F)$.

3.2. LEMMA. Let $A = F(\Lambda)$ be a projective Schur algebra over $F$, $\Lambda$ the spanning group, and $\Lambda/F^*$ abelian. Then the order of $[A]$ in $\text{Br}(F)$ divides $\text{exp}(\Lambda/F^*)$.

Proof. The argument is precisely the one used in the proof of Theorem 1.1 in [4]. Let us sketch the proof adapted to our needs. First it is shown that it is sufficient to consider $\Lambda/F^*$ a $p$-group. Next, if $1 \neq \Lambda/F^* \cong \mathbb{Z}_{p^{r_1}} \times \cdots \times \mathbb{Z}_{p^{r_t}}$ with $r_1 \geq r_2 \geq \cdots \geq r_t$, then $t \geq 2$ and $r_1 = r_2 (= r)$. The third step is to show that if $s_1, s_2$ are generators of $\mathbb{Z}_{p^{r_1}}, \mathbb{Z}_{p^{r_2}}$, respectively, and $u_{s_1}, u_{s_2}$ are elements in $\Lambda$ that are mapped to $s_1, s_2$ under the natural map, then the $F$-subalgebra of $A$ generated by $u_{s_1}, u_{s_2}$ is isomorphic to the $(F$-central$)$ symbol algebra $(u_{s_1}^{p^r}, u_{s_2}^{p^r})_{p^r}$ of degree $p^r$ (and therefore of order dividing $p^r$). Finally one shows that $A \cong (u_{s_1}^{p^r}, u_{s_2}^{p^r})_{p^r} \otimes_F F(\Lambda_0)$ where $\Lambda_0/F^*$ is abelian and $\text{exp}(\Lambda_0/F^*) \mid \text{exp}(\Lambda/F^*)$. The proof is then completed by induction on the dimension of $A$.

In view of the lemma above, the main theorem will be proved if we show that the exponent of the group $H/k(H_0)^*$ divides the number of roots of unity in $k$ (rather than the number of roots of unity in $k(H_0)$). So let us assume that the field $k$ contains a primitive $p^r$th root of unity but not a primitive $p^{r+1}$th root of unity, $r \geq 0$. We assume that $H$ contains an element $\sigma$ of order $p^{r+1}$ modulo $k(H_0)^*$ and get a contradiction. Recall that the order of $\sigma$ modulo $k^*$ is finite so taking a prime-to-$p$ power of $\sigma$ we can assume that the order of $\sigma$ modulo $k(H_0)^*$ is $p^{r+1}$ and its order modulo $k^*$ is a power of $p$. Consider the subalgebra $k(H_0, \sigma)$. It is commutative since $\sigma$ centralizes the field $k(H_0)$, and moreover $k(H_0, \sigma)$ is a field extension of $k(H_0)$ since $k(\Gamma)$ is reduced. The group $\Gamma$ acts on the field $k(H_0, \sigma)$
by conjugation and, as above, the fixed field must be \( k \) because otherwise the center of \( k(\Gamma') \) would be a proper extension of \( k \). The Galois group of \( k(H_0, \sigma) \) over \( k \) is a quotient of \( \Gamma'/\Gamma' \) and hence is abelian. This implies that every field extension of \( k \) contained in \( k(H_0, \sigma) \) is also abelian and in particular the field generated by \( \sigma \) over \( k \).

We analyze the extension \( k(\sigma)/k \) where \( \sigma \) satisfies \( \sigma^{p^{r+1}+t} = b \in k^* \), \( t \geq 0 \). A theorem due to Schinzel [9, Theorem 2], [5, p. 235] says that if \( k(\sigma)/k \) is an abelian extension then \( b^{p^r} = c^{p^{r+1}+t} \) for some \( c \in k^* \). Extracting \( p^{2r+1+t} \) roots of both sides of this equation yields \( b^{1/(p^{r+1}+t)} = \zeta c^{1/p^r} \) where \( \zeta \) is a \( p^{2r+1+t} \) root of unity. It follows that \( \sigma^{p^r} = \zeta c \) where \( \zeta \) is a \( p^{r+1+t} \) root of unity. To get a contradiction recall that the order of \( \sigma \) modulo \( k(H_0)^* \) is \( p^{r+1} \). This implies that \( k(H_0, \sigma^{p^r}) \) is a proper field extension of \( k(H_0) \) and in particular the subgroup \( \langle H_0, \sigma^{p^r} \rangle \) of \( \Gamma \) strictly contains \( H_0 \). But \( k(H_0, \sigma^{p^r}) = k(\zeta')(H_0) \), a cyclotomic extension of \( k \). This contradicts the maximality of \( H_0 \) in \( \Omega_k \) as desired.

We now prove Theorem 1.4. Let \( \alpha \in P\text{Nil}(k) \) of order \( n = p_1^{s_1} p_2^{s_2} \cdots \).

By [4, Prop. 2.8 (a)], it is sufficient to prove the theorem for \( n = p^s \), \( s > 0 \), where \( \alpha \) is represented by a projective Schur algebra \( k(\Gamma) \) of \( p \)-type, that is, \( \Gamma/k^* \) is a \( p \)-group, and by the proof of [4, Theorem 1.2], we may assume \( \Gamma' \) abelian. For this case we must show that the order of \( \text{res}_{k(H_0, \sigma^{p^s})}/k(\alpha) \) divides the number of \( p \)-power roots of unity contained in \( k \). If the \( p \)th roots of unity are not in \( k \), then as mentioned earlier, \( P\text{Nil}(k)\) is \( 0 \) and there is nothing to prove. We may therefore assume that \( k \) contains the \( p \)th roots of unity. We now simply modify the proof of Theorem 1 to suit the present situation. Since \( \Gamma'k^*/k^* \) is a \( p \)-group, the field extension \( k(\Gamma')/k \) is generated by \( p \)-power roots of unity. In the proof of Theorem 1.1 require in the definition of \( \Omega_k \) that \( k(T)/k \) be not only cyclotomic but generated by \( p \)-power roots of unity. In Lemma 3.1 (c), replace \( \mu \) by \( \mu_{p^\infty} \). Finally, we arrive at the contradiction that \( k(H_0, \sigma^{p^s}) \) is an extension of \( k \) generated by \( p \)-power roots of unity, and is strictly larger than \( k(H_0) \).

REFERENCES

1. E. Aljadeff and J. Sonn, Projective Schur division algebras are abelian crossed products, 
2. E. Aljadeff and J. Sonn, Projective Schur algebras have abelian splitting fields, J. Algebra 
   530–540.
4. E. Aljadeff and J. Sonn, Projective Schur algebras of nilpotent type are Brauer equivalent 