# ADMISSIBLE GROUPS, SYMMETRIC FACTOR SETS, AND SIMPLE ALGEBRAS

## R.A. MOLLIN

Mathematics Department
University of Calgary
T2N 1N4, Canada

ABSTRACT.  Let K be a field of characteristic zero and suppose that D is a K-division
algebra; i.e. a finite dimensional division algebra over K with center K.  In Mollin
[1] we proved that if K contains no non-trivial odd order roots of unity, then every
finite odd order subgroup of $D^*$, the multiplicative group of D, is cyclic.  The first
main result of this paper is to generalize (and simplify the proof of) the above.
Next we generalize and investigate the concept of admissible groups.  Finally we
provide necessary and sufficient conditions for a simple algebra, with an abelian
maximal subfield, to be isomorphic to a tensor product of cyclic algebras.  The
latter is achieved via symmetric factor sets.

## 1.  NOTATION AND PRELIMINARIES.

Let K be a field of characteristic zero.  We define the Schur subgroup S(K) of
B(K), the Brauer group of K, to be those equivalence classes which contain a simple
component of the group algebra KG for some finite group G.  We let [A] denote the
equivalence class of the K-central simple algebra A in B(K).  The notation A ~ B
means [A] = [B] in B(K).  When A ⊗ B is written, the tensor product is assumed to be
taken over the algebra in the left factor.  For most basic results pertaining to S(K)
the reader is referred to Yamada [2].

A crossed product algebra will be denoted (K/k,β) which is the central simple
k-algebra having K-basis $u_\sigma$ with $\sigma \in G(K/k)$, subject to: $u_\sigma u_\tau = \beta(\sigma,\tau)u_{\sigma\tau}$ and
$u_\tau x = x^\tau u_\tau$ where $x \in K$ and $\sigma,\tau \in G(K/k)$, the Galois group of K over k.  For further
information pertaining to crossed products the reader is referred to Reiner [3].

Finally we comment on notation.  If m is a positive integer with $m = p^a n$ where
the prime p does not divide n then $|m|_p = p^a$; i.e. $|m|_p$ denotes the p-part of m.  A
primitive $m^{th}$ root of unity will be denoted by $\varepsilon_m$.

## 2.  SUBGROUPS OF SIMPLE ALGEBRAS.

Let K be a field of characteristic zero.  The major thrust of this section is to
provide a generalization of Mollin [1, Theorem 3.6, p. 243].  To pave the road we
first need a definition and some preliminary results.

Let D be an E-division algebra for some field E, finite dimensional over K, and let n be a fixed positive integer. We say that D is (n,K)-adequate if there exists a K-division algebra B with K · I $\subseteq$ D $\subseteq$ $M_n$(B) where I is the identity of $M_n$(B), the full ring of n × n matrices with entries from B.

We need the following result which generalizes Mollin [1, Theorem 3.4, p. 242]. In what follows Aut(D) denotes the automorphism group of D.

THEOREM 2.1. Let E/K be finite Galois. If D is an (n,K)-adequate E-division algebra and $\sigma \in$ G(E/K) then $\sigma$ extends to Aut(D).

PROOF. Let A = $M_n$(B) where D is embedded in A. If C = $C_A$(E) denotes the centralizer of E is A then by Reiner [3, Corollary 7.14, p. 96] we have [C] = [B $\otimes_K$ E]. The remainder of the proof follows from this juncture exactly as the proof of Mollin [1, Theorem 3.4, p. 242].                                                      Q.E.D.

The following which is immediate generalizes Mollin [1, Corollary 3.5, p. 242].

COROLLARY 2.2. Let E/K be finite Galois, and let D be an (n,K)-adequate E-division algebra. If [D] $\in$ S(E), with exponent m, then $\epsilon_m$ is in K.

In what follows a subgroup of $M_n$(D) will mean a finite multiplicative subgroup of $M_n$(D). The following result is immediate from Hikari [4, propositions 1 and 2, pp. 369-370]. Note that if G is an abelian group expressible as a direct sum of cyclic groups $C_1 \oplus ... \oplus C_n$ with $|C_i|$ = $e_i$ such that $e_i | e_{i+1}$ for i = 1,2,...,n-1 and $e_n \neq$ 1 then we say that G has invariants of length n.

LEMMA 2.3. Suppose that G is a subgroup of $M_n$(D) where n $\leq$ p for the minimum odd prime divisor p of $|G|$. Then all odd Sylow subgroups of G are abelian with invariants of length less than or equal to n.

Now we need another definition. Given a K-division algebra D and a fixed positive integer n, suppose that G is a subgroup of $M_n$(D). We let V(G) = $\{\Sigma\ a_i g_i : a_i \in$ Q;$g_i \in$ G$\}$. V(G) is a Q subalgebra of $M_n$(D) and is, in fact, a direct summand of the group algebra QG. This generalizes the concept as used in Amitsur [5] for the case n = 1 wherein V(G) is a minimal division algebra containing G. Now we are in a position to prove the main result of this section.

THEOREM 2.4. Let n be a fixed positive integer and let D be a K-division algebra. If K contains no non-trivial odd order roots of unity then every odd order subgroup of $M_n$(D), with n < p for the minimum prime divisor of $|G|$, is abelian with invariants of length $\leq$ n.

PROOF. Suppose V(G) = $\overset{\oplus}{i} M_{n_i}$ ($D_i$) $\subseteq$ $M_n$(D). Thus $\overset{\Sigma}{i} n_i \leq$ n < p. But $n_i$ divides $|G|$, (see Curtis and Reiner [6, Chapter IV]). Hence, $n_i$ = 1 for each i. Now if $D_i$ is commutative for each i then G is abelian in which case we get the result from lemma 2.3. Thus we assume that $D_j$ is a (non-trivial) division algebra for some j. Then [$D_j$] has odd exponent, r > 1 say, in S(E) where E/Q is finite abelian (see Amitsur [5]). But $D_j \subseteq M_n$(D) so $D_j \otimes$ KE is (n,K)-adequate, and $D_j \otimes$ KE is a division algebra such that [$D_j \otimes$ KE] has exponent r in S(KE). By corollary 2.2, $\epsilon_r$ is in K, contradicting the hypothesis.                                                      Q.E.D.

3. ADMISSIBILITY

The following definitions generalize concepts introduced in Schacher [7]. Let K/k be a finite extension of fields. K is called (n,k)-adequate if and only if K is

a self-centralizing maximal subfield of $M_n(D)$ for some k-division ring D, and n is the smallest positive integer for which there is such an embedding as k-algebras, (see Reiner [3, Chapter 7]). A finite group G is called (n,k)-admissible if and only if there is a Galois extension K of k with G = G(K/k) and K is (n,K)-adequate. G is called totally n-admissible if and only if for each pair of number field K and k with K Galois over k and G = G(K/k) we have that K is (n,k)-adequate.

The reader should note that the concept of K-adequacy was used in [1] to prove that every finite odd order multiplicative subgroup of a division ring D is cyclic, whenever the center of D has no non-trivial odd order roots of unity, ([1, Theorem 3.6, p. 243]). Herein our extension from the K-adequacy concept to the (n,K)-adequacy concept tacitly allowed us to prove theorem 2.4 which generalized [ibid] since we were in a position to consider subgroups of $M_n(D)$ for a given fixed positive integer n. The mechanism for proving theorem 2.4 was the Q-subalgebra V(G) of $M_n(D)$. This mechanism opened the door for the use of lemma 2.3 and corollary 2.2.

The first result of this section generalizes Schacher [7, Theorem 2.8, p. 455], which is the n = 1 case. Also this proves Mollin [8, Theorem 3, p. 135].

THEOREM 3.1. Let n be a fixed positive integer dividing $|G|$. Then G is totally n-admissible if and only if every Sylow p-subgroup of G has an element of order $|G|_p / |n|_p$.

PROOF. Let G = G(K/k) for a given pair of number fields K and k. Suppose that $G_p$ is a Sylow p-subgroup of G and $\sigma \in G_p$ has order $|G|_p / |n|_p$. Let $M^{(p)}$ be the fixed field of $<\sigma>$; i.e. $G(K/M^{(p)}) = <\sigma>$. Therefore, by class field theory there are distinct $M^{(p)}$-primes $\hat{p}_1$ and $\hat{p}_2$ which are inert in K, and $p_1 = \hat{p}_1 \cap k \neq \hat{p}_2 \cap K = p_2$, (see Janusz [9, Chapter IV]). Define $[\Delta^{(p)}] \in B(k)$ by $\mathrm{inv}_{p_i}(\Delta^{(p)}) = (-1)^i / |\sigma|$ for i = 1,2; and $\mathrm{inv}_q(\Delta^{(p)}) = 0$ for all $q \neq p_i$.

Now for each $p||G|$ form such a $\Delta^{(p)}$ and let $\Delta$ be the k-division algebra $\bigotimes_{p||G|} \Delta^{(p)}$. Then K splits $\Delta$ and by Reiner [3, §28, pp. 237-241] n is the smallest positive integer such that K is a self-centralizing maximal subfield of $M_n(\Delta)$; i.e. K is (n,k)-adequate. Hence G is totally n-admissible.

Conversely suppose that G is totally n-admissible. Then if G = G(K/k) we have that K is embedded in $M_n(D)$ for some k-division ring D, with n being the smallest such positive integer. By Reiner, [3, ibid] we have that $n = |K:k| / \sqrt{|D:k|}$. Moreover, by Artin and Tate [10, p. 75] we may assume that K/k is unramified.

Now by Albert, [11, theorem 33, p. 150] we have $\sqrt{|D:k|}$ is equal to the least common multiple of the degrees $|K_{\hat{P}}:k_p|$ taken over all primes at which D has non-zero Hasse invariant. Thus there exists a K-prime $\hat{P}$ such that $|K_{\hat{P}}:k_p|_p = |D:k|_p$ for each p dividing $|K:k|$. Since $G(K_{\hat{P}}/k_p)$ is generated by the Froebenius automorphism of $\hat{P}$ in K/k then G must have an element of order $\sqrt{|D:k|}_p = |K:k|_p / |n|_p = |G|_p / |n|_p$ for each p dividing $|G|$.                                                        Q.E.D.

The following are immediate.

COROLLARY 3.2. Let n divide $|G|$. If G is totally n-admissible then G is metacyclic. In particular G is solvable.

COROLLARY 3.3.  For each pair of number fields K and k with K/k normal and
G = G(K/k) we have that the following are equivalent:

(1)  $|G|$ = $\ell$, the l.c.m. of the inertial degrees of all k-primes in K/k.

(2)  All Sylow p-subgroups of G are cyclic.

(3)  G is totally $\ell$-admissible nilpotent .

(4)  Let m,r be two relatively prime integers.  Put s = (r-1,m), t = m/s and $n_o$ = minimal integer satisfying $r^{n_o} \equiv 1 \pmod{m}$.  Then $G = \langle a,b : a^m = 1, b^{n_o} = a^t, b^{-1}ab = a^r \rangle$ where $|G|$ = $mn_o$ and g.c.d. $(n_o,t)$ = 1.

Now we consider the case where G is abelian.

THEOREM 3.4.  Let G be a finite abelian group.  Then G is (n,k)-admissible for some number field k and some positive integer n dividing $|G|$.

PROOF.  Schacher [7, Theorem 6.2, p. 465] guarantees that G = G(K/k) for some abelian extension K of k.  We must show that K is (n,k)-adequate.  Since G is abelian then there exists a subgroup of order n.  Let E be the fixed field of this subgroup.  Since H = G(E/k) is abelian then H is (1,k)-admissible by Schacher [7, ibid]; i.e. E is embedded as a maximal self-centralizing subfield of a k-division algebra $\Delta$.  Since K splits $\Delta$ then by Reiner [3, Chapter 7] K is embedded in $M_n(\Delta)$ as a self-centralizing maximal subfield with n as the least such positive integer.      Q.E.D.

Now suppose that G is finite abelian and $M_n(\Delta)$ is a K-central simple algebra with G = G(L/K) where L is a maximal subfield of $M_n(\Delta)$.  Thus $M_n(\Delta) \sim (L/K,\beta)$ for a suitable factor set $\beta$.  Now G = $\langle\sigma_1\rangle\times\langle\sigma_2\rangle\times...\times\langle\sigma_t\rangle$ where $\sigma_i$ has order $n_i$, say. It is natural to ask whether $(L/K,\beta)$ has a similar decomposition as a product of cyclic algebras of exponent $n_i$.  The following theorem yields a necessary and sufficient condition for such a decomposition to exist.  In what follows a __symmetric factor set__ $\beta$ means one such that $\beta(\sigma,\tau) = \beta(\tau,\sigma)$ for all $\sigma,\tau \in G$.  Moreover $L_i$ shall denote the fixed field $\prod_{j\neq i} \langle\sigma_j\rangle$.

THEOREM 3.5.  Let G be a finite abelian group.  Then G is (n,K)-admissible for some number field K and some n dividing $|G|$.  Suppose that A = $(L/K,\beta)$ is a K-central simple algebra with G = G(L/K).  Then A $\cong A_1 \otimes...\otimes A_t$ where each $A_i$ is cyclic K-central simple with maximal subfield $L_i$ if $\beta$ is symmetric.  Conversely we have the weaker result:  If A $\cong A_1 \otimes...\otimes A_t$ then $\beta$ is __cohomologous__ to a symmetric factor set.

PROOF.  Assume $\beta$ is symmetric.  Now each $\sigma \in G$ clearly extends to an inner automorphism of A: $\alpha \to u_\sigma \alpha u_\sigma^{-1}; \alpha \in A$.  Since $\beta(\sigma,\tau) = \beta(\tau,\sigma)$ for each $\sigma,\tau \in G$ then $u_\sigma u_\tau = u_\tau u_\sigma$ for each $\sigma,\tau \in G$.  These two facts imply that $h_i^{\sigma_j} = h_i$ for each i and j where $h_i = u_{\sigma_i}^{n_i}$.  Therefore $h_i \in K$ for each i, which implies $A_i = (L_i/K,h_i)$ is a cyclic crossed product algebra with maximal subfield $L_i$.

Now since L = $L_1 \times L_2 \otimes...\otimes L_t$ then n = $n_1 n_2...n_t$.  Since $\sigma = \sigma_1^{x_1}...\sigma_t^{x_1}$ then $u_\sigma = u_{\sigma_1}^{x_1}...u_{\sigma_t}^{x_t}$.  Therefore the map from A to $A_1 \otimes...\otimes A_t$ given by $u_\sigma \to u_{\sigma_1}^{x_1} \otimes...\otimes u_{\sigma_t}^{x_t}$ yields a K-algebra isomorphism.

Conversely assume $A \cong A_1 \otimes \ldots \otimes A_t$. Now by Reiner [3, Theorem (29.16),p. 249] $A_i \sim (L/K, \text{inf}^{(i)} h_i)$ where $\text{inf}^{(i)}$ denotes the inflation map from $L_i$ to $L$. Moreover $h_i$ is symmetric, so $\text{inf}^{(i)} h_i$ is symmetric. Since the factor set of $\text{inf}^{(1)} A_1 \otimes \ldots \otimes \text{inf}^{(t)} A_t$ is the multiplication of $\text{inf}^{(i)} h_i$ it follows that $\beta$ is cohomologous to a symmetric factor set.                                                              Q.E.D.

## REFERENCES

1. MOLLIN, R.A., Herstein's Conjecture, Automorphisms and the Schur group, Communications in Algebra 6(3), (1978), 237-248.

2. YAMADA, T., The Schur Subgroup of the Brauer Group, Lecture Notes in Math. No. 397, Springer-Verlag (1974).

3. REINER, I. Maximal Orders, Academic Press, New York, (1975).

4. HIKARI, M., Multiplicative p-Subgroups of Simple Algebras, Osaka J. Math. 10 (1973), 369-374.

5. AMITSUR, S., Finite Subgroups of Division Rings, Trans. Amer. Math. Soc. 80 (1955), 361-386.

6. CURTIS, C. and REINER, I., Representation Theory of Finite Groups and Associative Algebras, Wiley (Interscience), New York, (1962).

7. SCHACHER, M., Subfields of Division Rings I, J. Algebra 9 (1968), 451-477.

8. MOLLIN, R.A., Subgroups of Simple Algebras and the Zeta Function, C-R. Math. Rep. Acad. Sci. Canada, Vol. III(1981), No. 3, 133-137.

9. JANUSZ, G. J., Algebraic Number Fields, Academic Press, New York, (1973).

10. ARTIN, E., and TATE, J., Class Field Theory, Benjamin, New York, (1968).

11. ALBERT, A.A., Structure of Algebras, Amer. Math. Soc., Colloquium Publications, 24, (1968).