PACIFIC JOURNAL OF MATHEMATICS
Vol. 107, No. 2, 1983

UNIFORM DISTRIBUTION IN SUBGROUPS OF THE BRAUER GROUP OF AN ALGEBRAIC NUMBER FIELD

GARY R. GREENFIELD

We construct subgroups of the Brauer group of an algebraic number field whose member classes have Hasse invariants satisfying a rigid arithmetic structure — that of (relative) uniform distribution. After obtaining existence and structure theorems for these subgroups, we focus on the problem of describing algebraic properties satisfied by the central simple algebras in these subgroups. Key results are that splitting fields are determined up to isomorphism, and there exists a distinguished subgroup of central automorphisms which can be extended.

1. Introduction. Let K be an algebraic number field, and let $[A]$ denote the class of the finite dimensional central simple K-algebra A in the Brauer group $B(K)$ of K. The class $[A]$ is determined arithmetically by its Hasse invariants at the primes of K. Algebraic properties of A often impose severe but interesting arithmetic properties on its invariants. As evidence we cite the important work of M. Benard and M. Schacher [2] concerning the invariants when $[A]$ is in $S(K)$ the Schur subgroup of K, and the surprising result of G. Janusz [4] obtained in considering the problem of when an automorphism of K extends to A.

In this paper we offer a construction which gives rise to subgroups of $B(K)$ whose member classes have invariants which possess a rigid arithmetic structure — that of uniform distribution — then search for corresponding algebraic properties. Our construction is modeled after one given by R. Mollin [5] to study subgroups of $B(K)$ which contain $S(K)$.

In §2 we present our construction and establish a series of results which culminate in an existence theorem. In §3, we consider questions concerning the structure of our subgroups. In §4, we present our main result, which shows that the classes we consider have splitting fields which are determined up to isomorphism, and in fact we characterize such classes. Our final section incorporates the aforementioned work of Janusz to give a wholly different algebraic description to our classes.

For the general theory of central simple algebras we refer the reader to [1]. If $[A] \in B(K)$, then A is a matrix ring over a unique division ring D and the index of $[A]$ written ind$[A]$ is $\sqrt{[D:K]}$. Moreover, if ind$[A]$

has prime factorization $\prod p_i^{e_i}$, then $[A]$ has a unique primary decomposition $[A] = \prod [A_i]$ where $\text{ind}[A_i] = p_i^{e_i}$. We recall that when K is an algebraic number field the index of $[A]$ is equal to its exponent in $B(K)$.

We denote the Hasse invariant of $[A]$ at the prime $\mathfrak{Q}$ of K by $\text{inv}_{\mathfrak{Q}}[A]$. An extensive treatment of the classification of $B(K)$ by invariants may be found in [3] or [6]. We summarize a few key results. The Hasse invariant $\text{inv}_{\mathfrak{Q}}[A]$ is a fraction modulo one whose denominator when expressed in lowest terms is the $\mathfrak{Q}$-local index of $[A]$ written $\text{l.i.}_{\mathfrak{Q}}[A]$. We denote the completion of K at the prime $\mathfrak{Q}$ by $K_{\mathfrak{Q}}$. *Unless otherwise indicated congruences will be taken modulo one.*

THEOREM 1.1. *Let* $[A], [B] \in B(K)$, L *a finite extension of* K, *and* $\mathfrak{R}$ *an* L*-prime above the* K*-prime* $\mathfrak{Q}$. *Then*

(i) $\text{inv}_{\mathfrak{Q}}[A]^{-1} \equiv -\text{inv}_{\mathfrak{Q}}[A]$.

(ii) $\text{inv}_{\mathfrak{Q}}[A \otimes_K B] \equiv \text{inv}_{\mathfrak{Q}}[A] + \text{inv}_{\mathfrak{Q}}[B]$.

(iii) $\text{inv}_{\mathfrak{R}}[A \otimes_K L] \equiv [L_{\mathfrak{R}} : K_{\mathfrak{Q}}]\text{inv}_{\mathfrak{Q}}[A]$.

(iv) $\text{ind}[A] = \text{l.c.m.}_{\mathfrak{Q}}\{\text{l.i.}_{\mathfrak{Q}}[A]\}$.

THEOREM 1.2. *Let* $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_s$ *be primes of* K *and* $r_1, \ldots, r_s$ *rational numbers satisfying*:

(i) $\Sigma r_i \equiv 0$; *and*

(ii) $r_i \equiv 0$ *if* $\mathfrak{Q}_i$ *is complex and* $r_i \equiv 0$ *or* $\frac{1}{2}$ *if* $\mathfrak{Q}_i$ *is real.*

Then there exists $[A] \in B(K)$ *with* $\text{inv}_{\mathfrak{Q}_i}[A] \equiv r_i$ *for all* $i = 1, \ldots, s$ *and* $\text{inv}_{\mathfrak{Q}}[A] \equiv 0$ *otherwise.*

2. Uniform distribution. Let G be a subgroup of $\text{Aut}(K)$, the full automorphism group of K, and let F be the fixed field of G. Thus K/F is Galois with Galois group G. Fix a map c: $G \to Z$ and say c: $\sigma \to c_\sigma$.

DEFINITION 2.1. The class $[A] \in B(K)$ has *uniformly distributed invariants relative to* c if

$$\text{inv}_{\mathfrak{Q}}[A] \equiv c_\sigma \text{inv}_{\mathfrak{Q}^\sigma}[A]$$

for all primes $\mathfrak{Q}$ of K and all $\sigma \in G$.

Let $R(K/F, G, c)$ be the set of classes having uniformly distributed invariants relative to c. When no confusion arises we will denote this simply by $R(K)$. It is immediate from the definition that $[K] \in R(K)$. Moreover, $R(K)$ is a subgroup of $B(K)$ as the required closure properties may be verified easily using Theorem 1.1. We wish to show $R(K)$ respects

primary decomposition. This allows a basic reduction in proofs. We begin with an easy lemma:

LEMMA 2.2. *For* $i = 1, 2$ *let* $a_i, b_i \in Z$ *and* $m_i \in Z^{\text{pos}}$. *Suppose* $(m_1, m_2) = 1$. *Then*

$$\frac{a_1}{m_1} + \frac{a_2}{m_2} \equiv \frac{b_1}{m_1} + \frac{b_2}{m_2} \text{ if and only if } \frac{a_i}{m_i} \equiv \frac{b_i}{m_i}.$$

Proof. Assume

$$\frac{a_1}{m_1} + \frac{a_2}{m_2} \equiv \frac{b_1}{m_1} + \frac{b_2}{m_2}.$$

Then

$$\frac{a_1 - b_1}{m_1} \equiv \frac{b_2 - a_2}{m_2}$$

and since $(m_1, m_2) = 1$ we must have $a_i - b_i = k_i m_i$ for some $k_i \in Z$. This gives implication in one direction. The converse is trivial.

THEOREM 2.3. *Let* $[A] \in B(K)$ *have primary decomposition* $[A] = [A_1] \cdots [A_s]$. *Then* $[A] \in R(K)$ *if and only if* $[A_i] \in R(K)$ *for all* i.

Proof. Using induction, it will be enough to show that if $[A] = [B_1][B_2]$ with $\text{ind}[B_i] = m_i$ and $(m_1, m_2) = 1$, then $[A] \in R(K)$ implies each $[B_i] \in R(K)$. Let $\mathfrak{P}$ be a prime of K and $\sigma \in G$. Say $\text{inv}_{\mathfrak{P}}[B] \equiv a_i/m_i$ and $\text{inv}_{\mathfrak{P}^\sigma}[B_i] \equiv b_i/m_i$.

$$\begin{aligned} \text{We have } a_1/m_1 + a_2/m_2 &\equiv \text{inv}_{\mathfrak{P}}[B_1] + \text{inv}_{\mathfrak{P}}[B_2] \\ &\equiv \text{inv}_{\mathfrak{P}}[A] \\ &\equiv c_\sigma \cdot \text{inv}_{\mathfrak{P}^\sigma}[A] \\ &\equiv c_\sigma(\text{inv}_{\mathfrak{P}^\sigma}[B_1] + \text{inv}_{\mathfrak{P}^\sigma}[B_2]) \\ &\equiv \frac{c_\sigma b_1}{m_1} + \frac{c_\sigma b_2}{m_2}. \end{aligned}$$

From Lemma 2.2 we conclude $a_i/m_i \equiv c_\sigma b_i/m_i$ and the proof is complete.

The main goal of this section is to prove an existence theorem for classes in $R(K)$. To do so we require technical information concerning invariants and the values of the classifying map c.

LEMMA 2.4. *Let* $[A] \in R(K)$ *and assume the primes* $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ *of* K *lie above a common F-prime* $\mathfrak{P}$. *Then* $\text{inv}_{\mathfrak{Q}_1}[A] \equiv 0$ *if and only if* $\text{inv}_{\mathfrak{Q}_2}[A] \equiv 0$.

Proof. By symmetry it suffices to prove if $\text{inv}_{\mathfrak{Q}_1}[A] \equiv 0$ then $\text{inv}_{\mathfrak{Q}_2}[A] \equiv 0$. Since K/F is Galois, G acts transitively on the primes of K above $\mathfrak{P}$. Thus we may choose $\sigma \in G$ such that $\sigma(\mathfrak{Q}_2) = \mathfrak{Q}_1$. Then $\text{inv}_{\mathfrak{Q}_2}[A] \equiv c_\sigma \text{inv}_{\mathfrak{Q}_2^\sigma}[A] \equiv c_\sigma \text{inv}_{\mathfrak{Q}_1}[A] \equiv c_\sigma \cdot 0 \equiv 0$.

LEMMA 2.5. *If* $[A] \in R(K)$ *has index* m, *then* $(c_\sigma, m) = 1$ *for all* $\sigma \in G$.

Proof. If $m = 1$ there is nothing to prove. We assume $m > 1$ has prime factorization $m = \prod p_i^{e_i}$ so we need only show $(c_\sigma, p_i^{e_i}) = 1$ for all i. But $[A]$ has primary decomposition $[A] = \prod[A_i]$ where $\text{ind}[a_i] = p_i^{e_i}$ and thanks to Theorem 2.3 we know each $[A_i] \in R(K)$. Thus, replacing $[A]$ by each $[A_i]$ in turn, we are reduced to proving the lemma when $[A]$ has prime power index $p^e > 1$.

Let $\mathfrak{Q}$ be a prime of K with $\text{l.i.}_{\mathfrak{Q}}[A] = p^e$, so $\text{inv}_{\mathfrak{Q}}[A] \equiv a/p^e$ where $(a, p) = 1$. If $\sigma \in G$, then by Lemma 2.4 $\text{inv}_{\mathfrak{Q}^\sigma}[A] \not\equiv 0$ so we may write $\text{inv}_{\mathfrak{Q}^\sigma}[A] \equiv b/p^f$ where $1 \leq f \leq e$ and $(b, p) = 1$. Now, $a/p^e \equiv \text{inv}_{\mathfrak{Q}}[A] \equiv c_\sigma \text{inv}_{\mathfrak{Q}^\sigma}[A] \equiv c_\sigma b/p^f$ which tells us $e = f$ and $c_\sigma \not\equiv 0 \bmod p$, whence $(c_\sigma, p^e) = 1$.

The last line of the preceding proof suggests $[A] \in R(K)$ has common local indices, and we show now that this is indeed the case.

PROPOSITION 2.6. *If* $[A] \in R(K)$ *and* $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ *are primes of* K *above the F-prime* $\mathfrak{P}$ *then* $\text{l.i.}_{\mathfrak{Q}_1}[A] = \text{l.i.}_{\mathfrak{Q}_2}[A]$.

Proof. If $[A] = [K]$, all local indices are one, so we assume $[A]$ has index $m > 1$. As usual, we invoke primary decomposition to write $[A] = \prod[A_i]$. Since the indices of the $[A_i]$ are relatively prime, $\text{l.i.}_{\mathfrak{Q}_j}[A] = \prod_i \text{l.i.}_{\mathfrak{Q}_j}[A_i]$. Thus $\text{l.i.}_{\mathfrak{Q}_1}[A] = \text{l.i.}_{\mathfrak{Q}_2}[A]$ if and only if $\text{l.i.}_{\mathfrak{Q}_1}[A_i] = \text{l.i.}_{\mathfrak{Q}_2}[A_i]$ for all i. But each $[A_i] \in R(K)$ so we assume without loss of generality $[A] \in R(K)$ has prime power index $p^e > 1$.

There is no harm in assuming $\text{l.i.}_{\mathfrak{Q}_1}[A]$ is maximal among primes of K above $\mathfrak{P}$. Since $\text{l.i.}_{\mathfrak{Q}_1}[A] = 1$ if and only if $\text{inv}_{\mathfrak{Q}_1}[A] \equiv 0$, Lemma 2.4 gives the desired result in this case. Thus we assume $\text{l.i.}_{\mathfrak{Q}_1}[A] = p^f$ where $1 \leq f \leq e$ and write $\text{inv}_{\mathfrak{Q}_1}[A] \equiv a/p^f$ where $(a, p) = 1$. Choose $\sigma \in G$ such that $\sigma(\mathfrak{Q}_1) = \mathfrak{Q}_2$. Since $\text{l.i.}_{\mathfrak{Q}_2}[A]$ divides p^e and is not one, we must have $\text{l.i.}_{\mathfrak{Q}_2}[A] = p^g$ where $1 \leq g \leq f$ and therefore $\text{inv}_{\mathfrak{Q}_2}[A] \equiv b/p^g$ where

$(b, p) = 1$. We have $a/p^f \equiv \text{inv}_{\mathfrak{Q}_1}[A] \equiv c_\sigma \cdot \text{inv}_{\mathfrak{Q}_1^\sigma}[A] \equiv c_\sigma \text{inv}_{\mathfrak{Q}_2}[A] \equiv c_\sigma b/p^g$. But $(c_\sigma, p^e) = 1$ so $f = g$ and we are done.

We can now state and prove our existence theorem. If $m > 1$ is an integer we let π_m: $Z \to Z_m$ be the canonical ring homomorphism, and denote the group of units of Z_m by $Z_m^\cdot$.

THEOREM 2.7. *Fix $m > 1$. There exists $[A] \in R(K)$ of index m if and only if the map $\pi_m \circ c$: $G \to Z_m$ is a group homomorphism to a subgroup of $Z_m^\cdot$.*

Proof. Assume there exists $[A] \in R(K)$ of index m. From Lemma 2.5 we see $\pi_m \circ c$: $G \to Z_m^\cdot$ is well defined. We must show that if $\tau, \sigma \in G$ then $c_{\tau\sigma} \equiv c_\tau c_\sigma \bmod m$. For any prime $\mathfrak{Q}$ of K,

$$\begin{aligned} c_{\tau\sigma}\text{inv}_{\mathfrak{Q}^{\tau\sigma}}[A] &\equiv \text{inv}_{\mathfrak{Q}}[A] \equiv c_\sigma \text{inv}_{\mathfrak{Q}^\sigma}[A] \\ &\equiv c_\sigma c_\tau \text{inv}_{(\mathfrak{Q}^\sigma)^\tau}[A] \equiv c_\tau \cdot c_\sigma \text{inv}_{\mathfrak{Q}^{\tau\sigma}}[A] \end{aligned}$$

so $c_{\tau\sigma} \equiv c_\tau c_\sigma \bmod \text{l.i.}_{\mathfrak{Q}}[A]$. Theorem 1.1 now gives the congruence modulo m.

To prove the converse, we assume $\pi_m \circ c$ gives a homomorphism onto a subgroup I_m of $Z_m^\cdot$. Let H_m be the kernel so $G/H_m \cong I_m$ and say $[G: H_m] = r = |I_m|$ while $|H_m| = h$. Choose left coset representatives $\sigma_1, \ldots, \sigma_r$ of H_m in G, so each $\sigma \in G$ is expressed uniquely as $\sigma = \sigma_i \tau$ where $\tau \in H_m$. Letting K_m be the fixed field of H_m we have $[K: K_m] = h$ while $[K_m: F] = r$. Select finite primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ of F which split completely in K. Let $\mathfrak{R}_{ij}, j = 1, \ldots, r$, be the primes of K_m above $\mathfrak{P}_i$. Since $\sigma_1, \ldots, \sigma_r$ act transitively on these primes we may assume $\sigma_j(\mathfrak{R}_{i1}) = \mathfrak{R}_{ij}$. Let $\mathfrak{Q}_{ijk}$, $k = 1, \ldots, h$, be the primes of K above $\mathfrak{R}_{ij}$. For $j = 1, \ldots, r$ let $c_{\sigma_j}^{-1}$ be any integer representative of the multiplicative inverse of c_{σ_j} in $Z_m^\cdot$. Using Theorem 1.2 we construct $[A] \in B(K)$ with $\text{inv}_{\mathfrak{Q}_{ijk}}[A] \equiv c_{\sigma_j}^{-1}/m$ for all i, j, k and $\text{inv}_{\mathfrak{Q}}[A] \equiv 0$ otherwise. This is allowed as $\sum_{i,j,k} \text{inv}_{\mathfrak{Q}_{ijk}}[A] \equiv m \cdot h \sum_{j=1}^r c_{\sigma_j}^{-1}/m \equiv 0$. Clearly $[A]$ has index m, and we wish to show $[A] \in R(K)$. Fix j between 1 and r and $\sigma = \sigma_t \tau \in G$. If $\sigma_t H \cdot \sigma_j H = \sigma_s H$, then $c_{\sigma_t} c_{\sigma_j} \equiv c_{\sigma_s} \bmod m$, hence $c_{\sigma_t} c_{\sigma_s}^{-1} \equiv c_{\sigma_j}^{-1} \bmod m$. Also $\sigma(\mathfrak{Q}_{ijk}) = \sigma_t \tau(\mathfrak{Q}_{ijk}) = \sigma_t(\mathfrak{Q}_{ijk'}) = \mathfrak{Q}_{isk''}$. Now,

$$\begin{aligned} \text{inv}_{\mathfrak{Q}_{ijk}}[A] &\equiv \frac{c_{\sigma_j}^{-1}}{m} \equiv \frac{c_{\sigma_t} \cdot c_{\sigma_s}^{-1}}{m} \\ &\equiv c_{\sigma_t} \cdot \text{inv}_{\mathfrak{Q}_{isk''}}[A] \equiv c_{\sigma_t} c_\tau \text{inv}_{\mathfrak{Q}_{isk''}}[A] \\ &\equiv c_{\sigma_t \tau} \text{inv}_{\mathfrak{Q}_{ijk}^\sigma}[A] \equiv c_\sigma \text{inv}_{\mathfrak{Q}_{ijk}^\sigma}[A], \end{aligned}$$

and the theorem is proved.

For $m > 1$, call the map $\pi_m \circ c$ *admissible* if it is a group homomorphism to a subgroup of Z_m^*. Then a readily observable corollary is:

COROLLARY 2.8. *Let $m, n > 1$ and suppose $n \mid m$. If $\pi_m \circ c$ is admissible, then so is $\pi_n \circ c$.*

Proof. Use Theorem 2.7 to provide $[A] \in R(K)$ of index m. Evidently $[A]^{m/n} \in R(K)$ has index n, so a second application of Theorem 2.7 shows $\pi_n \circ c$ is admissible.

3. Classifying maps. We examine now how the structure of $R(K/F, G, c)$ is affected by the choice of a classifying map c, and offer some ideas concerning the construction of such maps. We begin with the rationale for why our classes are called uniformly distributed.

Algebras with uniformly distributed invariants were introduced in [**2**] as they helped characterize the classes in $S(K)$, the Schur subgroup of $B(K)$, when K/Q is abelian [**2**, Theorem 1]. A generalization to the case K/F Galois is found in [**5**], where $U_F(K)$ the uniform distribution group of K relative to F is formulated and studied.

The principle of uniform distribution says that invariants of a class at primes of K above a fixed F-prime should yield the same local indices and occur equally often. That this holds for $R(K)$ will be shown by slightly modifying some results concerning $U_F(K)$ found in [**5**]. In fact many statements true for $U_F(K)$ have suitable analogs for $R(K)$. Let us fix notation.

Let $[A] \in R(K)$ have index greater than one. Suppose $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_v$ are the K-primes above the F-prime $\mathfrak{P}$ all having common local index $m > 1$. Since m divides the index of $[A]$, the map $\pi_m \circ c$ is admissible. We let I_m be its image, H_m its kernel, and K_m the fixed field of H_m. Finally, assume $\operatorname{inv}_{\mathfrak{Q}_1}[A] \equiv r/m$ where $0 < r < m$ and $(r, m) = 1$. We have (compare [**5**, Theorem 2.3 and Corollaries 2.5 and 2.6]):

THEOREM 3.1. (i) *$\mathfrak{P}$ is split completely in K_m.*

(ii) $\operatorname{inv}_{\mathfrak{Q}_i}[A] \equiv \operatorname{inv}_{\mathfrak{Q}_j}[A]$ *if and only if* $\mathfrak{Q}_i \cap K_m = \mathfrak{Q}_j \cap K_m$.

(iii) *The invariants at primes of K above $\mathfrak{P}$ are of the form t/m where t is in the coset rI_m in Z_m^*. All such values occur, and they occur equally often.*

Proof. Let $\mathfrak{Q}$ be a prime of K above $\mathfrak{P}$, $D_{\mathfrak{Q}}$ the decomposition group at $\mathfrak{Q}$, and $Z_{\mathfrak{Q}}$ the fixed field of $D_{\mathfrak{Q}}$.

(i) If $\sigma \in D_{\mathfrak{Q}}$, then $\operatorname{inv}_{\mathfrak{Q}}[A] \equiv c_\sigma \operatorname{inv}_{\mathfrak{Q}^\sigma}[A] \equiv c_\sigma \operatorname{inv}_{\mathfrak{Q}}[A]$ which forces $c_\sigma \equiv 1 \bmod m$ and thus $\sigma \in H_m$. Therefore K_m is a subfield of $Z_{\mathfrak{Q}}$, and so

the K_m-prime $\mathfrak{R} = \mathfrak{Q} \cap K_m$ is a prime above $\mathfrak{P}$ with relative and ramification degrees equal one. But K_m is normal over F so all extensions of $\mathfrak{P}$ to K_m must satisfy this property, hence $\mathfrak{P}$ is split completely in K_m.

(ii) For $\sigma \in G$, $\text{inv}_{\mathfrak{Q}}[A] \equiv \text{inv}_{\mathfrak{Q}^\sigma}[A]$ if and only if $c_\sigma \equiv 1 \pmod m$ which is true if and only if $\sigma \in H_m$. On the other hand, since $\mathfrak{P}$ is split completely in K_m, $\mathfrak{Q} \cap K_m = \mathfrak{Q}^\sigma \cap K_m$ if and only if $\sigma \in H_m$.

(iii) That each invariant has value t/m of the prescribed form and all such values occur follows easily from the definition of $R(K)$ and the fact that $\pi_m \circ c$ is onto I_m. Using K_m for $F(\varepsilon_m)$ and H_m for H in the proof of [**5**, Corollary 2.6] shows each value occurs $[H_m : D_{\mathfrak{Q}}]$ times.

We should also notice at this point that under a suitable choice for the map c we can almost recoup $U_F(K)$. Let $B_n(K)$ be the subgroup of $B(K)$ consisting of classes $[A]$ for which $[A]^n = [K]$.

PROPOSITION 3.2. *Let $\varepsilon = \varepsilon_n$ be the largest nth root of unity in K. Define c: $G \to Z$ by letting $\sigma(\varepsilon) = \varepsilon^{c_\sigma}$ where $0 < c_\sigma < n$ for all $\sigma \in G$. Then $R(K/F, G, c) = U_F(K)$ unless c is trivial in which case $R(K/F, G, c) \cap B_n(K) = U_F(K)$.*

Proof. Clearly K contains a primitive mth root of unity if and only if $m \mid n$. Notice that $\varepsilon^{n/m}$ serves as a primitive mth root of unity and, moreover, $\sigma(\varepsilon^{n/m}) = (\varepsilon^{n/m})^{c_\sigma}$. Next, observe $\pi_m \circ c$ is admissible if and only if $m \mid n$ unless c is trivial in which case it is admissible for all m. Now, examining the definition of $U_F(K)$ [**5**, p. 245] we find we may use c_σ for b and conclude $U_F(K) = R(K/F, G, c)$ unless c is trivial in which case bounding of exponents takes place in $U_F(K)$ but not $R(K/F, G, c)$, so our assumption on ε insures $R(K/F, G, c) \cap B_n(K) = U_F(K)$.

We have not been able to determine completely the role the classifying map c plays in determining the structure of $R(K/F, G, c)$; however with minimal information on the values of c we can give some idea of the size of $R(K/F, G, c)$. The following will be useful for the discussion.

LEMMA 3.3. *Suppose $\pi_m \circ c$ is admissible. Fix $[A] \in R(K/F, G, c)$ of index m. Then $\pi_m \circ c$ is trivial if and only if $[A]$ has identically distributed invariants viz., for any prime $\mathfrak{P}$ of F and any extensions $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ of $\mathfrak{P}$ to K, $\text{inv}_{\mathfrak{Q}_1}[A] \equiv \text{inv}_{\mathfrak{Q}_2}[A]$.*

Proof. If $\pi_m \circ c$ is trivial this is immediate from the definition. If $[A]$ has identically distributed invariants, we invoke primary decomposition, to reduce to proving the converse under the assumption m is a power of a

prime. Then choosing a prime $\mathfrak{Q}$ of K with $\text{l.i.}_{\mathfrak{Q}}[A] = m$, we have $c_\sigma \text{inv}_{\mathfrak{Q}}[A] \equiv \text{inv}_{\mathfrak{Q}}[A]$ for all $\sigma \in G$ so $c_\sigma \equiv 1 \bmod m$ for all $\sigma \in G$ as desired.

It is obvious from the definition of $R(K/F, G, c)$ and Lemma 2.4 that if zero is in $\text{Im}(c)$, the image of c, then $R(K/F, G, c)$ is trivial. Unfortunately, even if we rule out this possibility, a map c can still induce a trivial group. The following example highlights the obstruction.

EXAMPLE 3.4. Let K/F be Galois with $[K: F] = 3$. Say the Galois group G of K/F is $G = \{\sigma_1, \sigma_2, \sigma_3\}$, and define c: $G \to Z$ by $c(\sigma_i) = i$. Then $\pi_m \circ c$ has zero divisors if 2 or 3 divides m, and is never a subgroup of Z_m^* for $m \geq 5$ as $4 \notin \text{Im}(c)$. By the existence theorem $R(K/F, G, c)$ must be trivial.

Other peculiarities arise when $\text{Im}(c) \subset \{1, -1\}$. Our next proposition handles this eventually.

PROPOSITION 3.5. *Suppose* $\text{Im}(c) \subset \{1, -1\}$. *If c is a homomorphism then $R(K/F, G, c)$ contains a class of index m for every $m > 1$. Otherwise, $R(K/F, G, c)$ is a nontrivial subgroup of $B_2(K)$.*

Proof. In any event, $\pi_2 \circ c$ is admissible so $R(K/F, G, c)$ must contain classes of index 2. If $\pi_m \circ c$ is admissible for some $m > 2$, then $H_m = (\pi_m \circ c)^{-1}(1) = c^{-1}(1)$ is a subgroup of G so c itself must be a homomorphism. Put another way, $\pi_m \circ c$ is admissible for all $m \geq 2$ or just $m = 2$ according as c is or is not a homomorphism. An application of Theorem 2.7 finishes the proof.

In fact we can say slightly more when $\text{Im}(c) \subset \{1, -1\}$. If c is a homomorphism, then it is not too difficult to show $R(K/F, G, c)$ contains divisible subgroups. While if c is not a homomorphism, Lemma 3.3 gives a precise description of the classes in $R(K/F, G, c)$ — they are those classes in $B_2(K)$ such that for any prime $\mathfrak{P}$ of F either all extensions to K yield invariant 0 or all yield invariant $\frac{1}{2}$. We complete our discussion of size with:

THEOREM 3.6. *If there exists $\sigma \in G$ such that $|c_\sigma| > 1$, then $R(K/F, G, c) \subset B_m(K)$ for some $m > 1$* i.e., *$R(K/F, G, c)$ has bounded exponent.*

Proof. Let n be the exponent of G, and set $M = \max_{\tau \in G}\{|c_\tau|^n\} + 1$. Since $|c_\sigma| > 1$, $M > 1$. It suffices to show that if $[A] \in R(K/F, G, c)$ then $N = \operatorname{ind}(A) \leq M$. A routine induction shows $\operatorname{inv}_{\mathfrak{Q}}[A] \equiv c_\tau^n \operatorname{inv}_{\mathfrak{Q}}[A]$, and hence $\text{l.i.}_{\mathfrak{Q}}[A] \mid c_\tau^n - 1$, for all primes $\mathfrak{Q}$ of K and all $\tau \in G$. As N is the least common multiple of these local indices $N \mid c_\tau^n - 1$. We then write $|c_\sigma^n - 1| = k_\sigma N$ with $k_\sigma > 0$ and use the inequality $0 < |c_\sigma^n - 1| < |c_\sigma^n| + 1 \leq M$ to see $N \leq M$.

Given K/F, and hence G, we wish to show how to construct maps c so that $R(K/F, G, c)$ is nontrivial and has bounded exponent. To do this we must construct c so that $|c_\sigma| > 1$ for some $\sigma \in G$ and $\pi_m \circ c$ is admissible for some $m > 1$. Note that when $\pi_m \circ c$ is admissible its kernel must contain G' the commutator subgroup of G.

THEOREM 3.7. *Let K be a Galois extension of F with Galois group G. Let H be a subgroup of G containing G'. There exists a map $c\colon G \to Z^{\text{pos}}$ and an integer $m > 1$ such that $\pi_m \circ c$ is admissible with kernel H. For this map, $R(K/F, G, c)$ is nontrivial and has bounded exponent.*

Proof. If $H = G$, select $m > 1$ and set $c_\sigma = m + 1$ for all $\sigma \in G$. Then $\pi_m \circ c$ is trivial and $c_\sigma > 1$ so we are done. Thus we assume $H \neq G$ and write the abelian group G/H as a direct product of cyclic groups, say $G/H = C(n_1) \times C(n_2) \times \cdots \times C(n_r)$ where $C(n_i)$ is a cyclic group of order n_i. Using Dirichlet's Theorem on primes in an arithmetic progression, we may select distinct primes $p_1, \ldots, p_r$ such that $p_i \equiv 1 \bmod n_i$. Then $Z_{p_i}^*$ is cyclic of order $p_i - 1$ and has a cyclic subgroup of order n_i. Choosing integer representatives of this subgroup allows us to construct a map $c_i\colon C(n_i) \to Z^{\text{pos}}$ with the property that $\pi_{p_i} \circ c_i$ is an isomorphism. Now, using the Chinese Remainder Theorem, we can lift to a map $c\colon G/H \to Z^{\text{pos}}$ such that $\pi_{p_i} \circ c$ is admissible with kernel $\prod_{j \neq i} C(n_j)$. Finally, by keeping the map constant on cosets, we lift to a map $c\colon G \to Z^{\text{pos}}$ which clearly has the property that $\pi_m \circ c$ is admissible with kernel H when $m = \prod p_i$.

As we mentioned previously the classifying map c is not fully understood. An example will help illustrate the subtleties that may occur.

EXAMPLE 3.8. Let $F = Q$ and $K = Q(i, 4\sqrt{2})$. Then G is the Dihedral group of order 8. With presentation $\langle r, f \mid r^4, f^2, fr = r^3 f \rangle$, G consists of elements $r^i f^j$ where $i = 0, 1, 2, 3$ and $j = 0, 1$. The commutator subgroup

of G is $\langle r^2 \rangle$. Consider the maps $c_1, c_2 \colon G \to Z$ given by

$$c_1, c_2 \colon e, r^2 \to 1$$

$$\begin{aligned} c_1 &\colon r, r^3 \to -1, & c_2 &\colon r, r^3 \to -6, \\ c_1 &\colon f, r^2 f \to 6, & c_2 &\colon f, r^2 f \to -1, \\ c_1 &\colon rf, r^3 f \to -6, & c_2 &\colon rf, r^3 f \to 6. \end{aligned}$$

Independent of i, $\pi_m \circ c$ is admissible if and only if $m = 5$, 7, or 35. Moreover the image is the same in all cases and the kernel is G' when $m = 35$. The groups $R(K/F, G, c_i)$ have the same exponent but not the same classes. If would be interesting to know if, apart from the obvious bijection which preserves indices, there are any further relationships.

4. Common local indices. In this section we characterize by local indices a splitting criterion for classes $[A] \in B(K)$. Assume for the time being that F is merely a proper subfield of the algebraic number field K.

DEFINITION 4.1. The class $[A] \in B(K)$ has *common local indices relative to* F if for any prime $\mathfrak{P}$ of F and any extensions $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ of $\mathfrak{P}$ to K, $\text{l.i.}_{\mathfrak{Q}_1}[A] = \text{l.i.}_{\mathfrak{Q}_2}[A]$.

Let $C(K/F)$ be the set of classes with common local indices relative to F. It is clear that $[K] \in C(K/F)$ and if $[A] \in C(K/F)$ then $[A]^i \in C(K/F)$ for all $i \in Z$. We shall show $C(K/F)$ respects primary decomposition of classes, but first it is important to notice the:

PROPOSITION 4.2. *The set $C(K/F)$ is never a subgroup of $B(K)$.*

Proof. Let $[K\colon F] = m \geq 2$. Select finite primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_{m+1}$ of F which split completely in K, and let $\mathfrak{Q}_{ij}$ where $j = 1, \ldots, m$ be the primes of K above $\mathfrak{P}_i$. Via Theorem 1.2 we construct algebras $[A]$, $[B] \in B(K)$ whose nonzero invariants satisfy $\text{inv}_{\mathfrak{Q}_{ij}}[A] \equiv 1/(m+1)$ for all i, j; $\text{inv}_{\mathfrak{Q}_{ij}}[B] \equiv 1/(m+1)$ if $j < m$, and $\text{inv}_{\mathfrak{Q}_{im}}[A] \equiv -1/(m+1)$. By inspection $[A]$, $[B] \in C(K/F)$ and since $\text{inv}_{\mathfrak{Q}_{ij}}[A \otimes_K B] \equiv 2/(m+1)$ if $j < m$ and zero otherwise, we have $\text{l.i.}_{\mathfrak{Q}_{ij}}[A \otimes_K B] > 1$ if $j < m$ while $\text{l.i.}_{\mathfrak{Q}_{im}}[A \otimes_K B] = 1$. Thus $[A \otimes_K B] \notin C(K/F)$.

Once more the key to working in $C(K/F)$ is to use primary decomposition, so we prove:

THEOREM 4.3. *Let $[A] \in B(K)$ have index greater than one and primary decomposition $[A] = [A_1] \cdots [A_r]$. Then $[A] \in C(K/F)$ if and only if $[A_i] \in C(K/F)$ for all i.*

Proof. Let $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ be primes of K above a common F-prime. Primary decomposition promises $(\text{l.i.}_{\mathfrak{Q}_i}[A_j],\ \text{l.i.}_{\mathfrak{Q}_i}[A_k]) = 1$ for $j \neq k$ and that $\text{l.i.}_{\mathfrak{Q}_i}[A] = \prod_j \text{l.i.}_{\mathfrak{Q}_i}[A_j]$. This forces $\text{l.i.}_{\mathfrak{Q}_1}[A] = \text{l.i.}_{\mathfrak{Q}_2}[A]$ if and only if $\text{l.i.}_{\mathfrak{Q}_1}[A_j] = \text{l.i.}_{\mathfrak{Q}_2}[A_j]$ for all j.

Assume now that K/F is Galois with Galois group G, a nontrivial subgroup of $\text{Aut}(K)$. After Proposition 2.6, we see $R(K/F, G, c) \subset C(K/F)$. Thus our next theorem, the principal theorem of this paper, provides an algebraic description of the classes in $R(K)$. Denote by $\tilde{F}$ a fixed algebraic closure of F.

THEOREM 4.4. *Let $[A] \in B(K)$. Then $[A] \in C(K/F)$ if and only if whenever a finite extension L of K is a splitting field for $[A]$ and $\tau\colon L \to \tilde{F}$ is an isomorphism such that $\tau|_K \in G$, then $\tau(L)$ is a splitting field for $[A]$.*

Proof. Assume $[A] \in C(K/F)$ and L, τ satisfy the above hypotheses. Let $\tau|_K = \sigma \in G$. If $\mathfrak{Q}$ is a prime of K with $\text{inv}_{\mathfrak{Q}}[A] \not\equiv 0$, we must show $\text{inv}_{\mathfrak{R}}[A \otimes_K \tau(L)] \equiv 0$ for all primes $\mathfrak{R}$ of L extending $\mathfrak{Q}$. But

$$\text{inv}_{\mathfrak{R}}[A \otimes_K \tau(L)] \equiv \text{inv}_{\mathfrak{Q}}[A] \cdot [\tau(L)_{\mathfrak{R}} : K_{\mathfrak{Q}}]$$

so it suffices to show $\text{l.i.}_{\mathfrak{Q}}[A] \mid [\tau(L)_{\mathfrak{R}} : K_{\mathfrak{Q}}]$. Now $\tau^{-1}(\mathfrak{R})$ is a prime of L lying above $\tau^{-1}(\mathfrak{R}) \cap K = \sigma^{-1}(\mathfrak{Q})$. Clearly $\mathfrak{Q}$ and $\sigma^{-1}(\mathfrak{Q})$ lie above a common F-prime so $\text{l.i.}_{\mathfrak{Q}^{\sigma^{-1}}}[A] = \text{l.i.}_{\mathfrak{Q}}[A]$. Also, L splits $[A]$, hence $\text{l.i.}_{\mathfrak{Q}^{\sigma^{-1}}}[A] \mid [L_{\mathfrak{R}^{\tau^{-1}}} : K_{\mathfrak{Q}^{\sigma^{-1}}}]$. Finally, the fact that $[L_{\mathfrak{R}^{\tau^{-1}}} : K_{\mathfrak{Q}^{\sigma^{-1}}}] = [\tau(L)_{\mathfrak{R}} : K_{\mathfrak{Q}}]$ establishes the result.

For the converse, let $[A] \in B(K)$ have primary decomposition $[A] = \prod[A_i]$. Evidently the splitting property holds for $[A]$ if and only if it holds for each $[A_i]$. This observation coupled with the previous theorem allows us to reduce to the case where $[A]$ has prime power index $p^e > 1$. Suppose, for the purpose of contradiction, that the splitting property holds for $[A]$ but $[A] \notin C(K/F)$. This means there is a prime $\mathfrak{P}$ of F whose extensions $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_s$ where $s \geq 1$ of K when ordered so that $\text{l.i.}_{\mathfrak{Q}_i}[A] \leq \text{l.i.}_{\mathfrak{Q}_j}[A]$ for $i < j$ satisfy $p_1^{e_1} = \text{l.i.}_{\mathfrak{Q}_1}[A] < \text{l.i.}_{\mathfrak{Q}_s}[A] = p^{e_s}$. Choose $\sigma \in G$ such that $\sigma(\mathfrak{Q}_1) = \mathfrak{Q}_s$. Let $\mathfrak{S}_1, \ldots, \mathfrak{S}_m$ be the (finitely) many primes of K not over $\mathfrak{P}$ at which $[A]$ has nonzerro invariants. From the Grünwald-Wang Theorem there exists a cyclic extension L of K such that if $\mathfrak{R}_i$ is an L-prime above $\mathfrak{Q}_i$ then

$$\left[L_{\mathfrak{R}_i} : K_{\mathfrak{Q}_i}\right] = \begin{cases} p^{e_1} & \text{for } i = 1, \\ p^{e_s} & \text{for } i > 1 \end{cases}$$

while if $\mathfrak{T}_j$ is an L-prime above $\mathfrak{S}_j$ then

$$\left[L_{\mathfrak{T}_j}: K_{\mathfrak{S}_j}\right] = \begin{cases} p^e & \text{for } \mathfrak{S}_j \text{ finite,} \\ 2 & \text{for } \mathfrak{S}_j \text{ real.} \end{cases}$$

It is immediate that L splits $[A]$. Let τ: $L \to \tilde{F}$ be any isomorphism extending σ. If $\mathfrak{U}$ is a prime of $\tau(L)$ above $\mathfrak{Q}_s$, then $[\tau(L)_{\mathfrak{U}}: K_{\mathfrak{Q}_s}] = [L_{\mathfrak{U}\tau^{-1}}: K_{\mathfrak{Q}_s^{\sigma^{-1}}}] = [L_{\mathfrak{U}\tau^{-1}}: K_{\mathfrak{Q}_1}] = p^{e_1}$. Writing $\operatorname{inv}_{\mathfrak{Q}_s}[A] \equiv a/p^{e_s}$ where $(a, p) = 1$ and recalling that $e_1 < e_s$ we have

$$\operatorname{inv}_{\mathfrak{U}}[A \otimes_K \tau(L)] \equiv \operatorname{inv}_{\mathfrak{Q}_s}[A] \cdot \left[\tau(L)_{\mathfrak{U}}: K_{\mathfrak{Q}_s}\right] \equiv \frac{a}{p^{e_s}} \cdot p^{e_1} \not\equiv 0,$$

whence $\tau(L)$ is not a splitting field for $[A]$. This gives a contradiction, and the proof is complete.

5. Extensions of automorphisms. Let K be an algebraic number field, and A a K-algebra. Following [**4**], we denote by $I(A)$ the subgroup of $\operatorname{Aut}(K)$ consisting of those σ which satisfy $\operatorname{inv}_{\mathfrak{Q}}[A] \equiv \operatorname{inv}_{\mathfrak{Q}^\sigma}[A]$ for all K-primes $\mathfrak{Q}$; and by $\operatorname{Aut}(K; A)$ the subgroup of $\operatorname{Aut}(K)$ consisting of automorphisms which can be extended to A. Then [**4**, Theorem 3] $I(A) = \operatorname{Aut}(K; A)$. In this final section we obtain algebraic information about classes $[A] \in R(K/F, G, c)$ by considering $\operatorname{Aut}(K; A)$. Recall that when $\pi_m \circ c$ is admissible, H_m is its kernel.

THEOREM 5.1. *If* $[A] \in R(K/F, G, c)$ *has index* $m > 1$, *then* $\operatorname{Aut}(K; A) \cap G = H_m$.

Proof. We need only show $I(A) \cap G = H_m$. If $\sigma \in H_m$, write $c_\sigma = 1 + k_\sigma m$. Then for any prime $\mathfrak{Q}$ of K, $\text{l.i.}_{\mathfrak{Q}^\sigma}[A] \mid m$ so $\operatorname{inv}_{\mathfrak{Q}}[A] \equiv c_\sigma \operatorname{inv}_{\mathfrak{Q}^\sigma} \equiv \operatorname{inv}_{\mathfrak{Q}^\sigma}[A]$ and this gives containment in one direction. Suppose now $\sigma \in I(A) \cap G$. From $c_\sigma \operatorname{inv}_{\mathfrak{Q}^\sigma}[A] \equiv \operatorname{inv}_{\mathfrak{Q}}[A] \equiv \operatorname{inv}_{\mathfrak{Q}^\sigma}[A]$ we see $c_\sigma \equiv 1 \bmod \text{l.i.}_{\mathfrak{Q}}[A]$. Theorem 1.1 part (iv) gives $c_\sigma \equiv 1 \bmod m$ whence $\sigma \in H_m$.

COROLLARY 5.2. *Suppose* $R(K/F, G, c)$ *is not trivial.*

(i) *If* c *is a homomorphism with kernel* H *then* $\operatorname{Aut}(K; A) \cap G = H$ *for all* $[A] \in R(K/F, G, c)$.

(ii) *If* c *is not a homomorphism, then* $H_m \subset \operatorname{Aut}(K; A)$ *for all* $[A] \in R(K/F, G, c)$ *where* m *is the exponent of* $R(K/F, G, c)$.

Proof. Let $[A] \in R(K/F, G, c)$ have index $n > 1$. By the previous theorem, $H_n = G \cap \operatorname{Aut}(K; A)$. If c is a homomorphism, then $H_n = H$

and we are done; if not, by Theorem 3.6 m is well-defined and $n \mid m$ so $H_m \subset H_n$ as required.

REMARK. Recalling that $G' \subset H_m$ and using Theorem 3.7 one may construct classifying maps c such that $G' \subset \mathrm{Aut}(K; A)$ for all $[A] \in R(K/F, G, c)$. All examples known to us also allow the construction of a map c such that $H \subseteq \mathrm{Aut}(K; A)$ for all $[A] \in R(K/F, G, c)$ where H is any fixed subgroup with $G' \subset H \subset G$.

REFERENCES

[1] A. Albert, *Structure of algebras*, Amer. Math. Soc., New York, 1939.
[2] M. Benard and M. Schacher, *The Schur subgroup II*, J. Algebra, **22** (1972), 378–385.
[3] M. Deuring, *Algebra*, Springer-Verlag, New York/Berlin, 1968.
[4] G. Janusz, *Automorphism Groups of Simple Algebras and Group Algebras*, Lecture Notes in Pure and Applied Math., **37**, Dekker, 1978, 381–388.
[5] R. Mollin, *Generalized uniform distribution of Hasse invariants*, Comm. in Algebra **5** (1977), 245–266.
[6] I. Reiner, *Maximal Orders*, Academic Press, New York, 1975.

Received January 27, 1981.

WAYNE STATE UNIVERSITY
DETROIT, MI 48202
Current address: University of Richmond
Richmond, VA 23173