

Uniform Distribution Classified.

Mollin, Richard

in: Mathematische Zeitschrift, volume: 165

pp. 199 - 212



Terms and Conditions

The Göttingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes.

Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept there Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact:

Niedersächsische Staats- und Universitätsbibliothek

Digitalisierungszentrum

37070 Goettingen

Germany

Email: gdz@www.sub.uni-goettingen.de

Purchase a CD-ROM

The Goettingen State and University Library offers CD-ROMs containing whole volumes / monographs in PDF for Adobe Acrobat. The PDF-version contains the table of contents as bookmarks, which allows easy navigation in the document. For availability and pricing, please contact:

Niedersaechisische Staats- und Universitaetsbibliothek Goettingen - Digitalisierungszentrum

37070 Goettingen, Germany, Email: gdz@www.sub.uni-goettingen.de

Uniform Distribution Classified

Richard Mollin

Department of Mathematics, McMaster University, Hamilton, Ontario L8S 4K1, Canada

Introduction

Let K/F be finite Galois where F is an algebraic number field, and let $[A]$ denote the class of the central simple K -algebra A in the Brauer group $B(K)$ of K . We define $U_F(K)$ to be the subset of $B(K)$ consisting of those classes $[A]$ such that:

- (0.1) If the index of A is m then ε_m , a primitive m^{th} root of unity is in K , and
 (0.2) If \mathcal{P} is a K -prime lying over the F -prime \mathfrak{p} and $\sigma \in G(K/F)$, the Galois group of K/F , with $\varepsilon_m^\sigma = \varepsilon_m^{b\sigma}$ then the Hasse \mathcal{P} invariant of A satisfies:

$$\text{inv}_{\mathcal{P}}(A) \equiv b \text{inv}_{\mathcal{P}} \sigma(A) \pmod{1}.$$

$U_F(K)$ is a group called the *group of algebras with uniformly distributed invariants, over K relative to F* .

We note that whenever $[A] \in U_F(K)$ and $\hat{\mathfrak{q}}$ and $\hat{\mathfrak{q}}_1$ are K -primes above the F -prime \mathfrak{q} then $A \otimes_K K_{\hat{\mathfrak{q}}}$ and $A \otimes_K K_{\hat{\mathfrak{q}}_1}$ have the same index. We denote the common value of the indices $A \otimes_K K_{\hat{\mathfrak{q}}}$ for all K -primes $\hat{\mathfrak{q}}$ above \mathfrak{q} by $\text{ind}_{\mathfrak{q}}(A)$, called the \mathfrak{q} -local index of A , (see Mollin [13]).

The Schur subgroup $S(K)$ of $B(K)$ consists of those algebra classes containing a K -isomorphic copy of a simple summand of KG for some finite group G . We note that $S(K)$ is in fact a subgroup of $U_F(K)$, (see Mollin [13]). We studied the relationship between $U_F(K)$ and $S(K)$ in [9–16].

The main result of this paper is the classification of the division algebra representatives of the classes of $U(K)$ the absolute uniform distribution group for K , (see Mollin [13]), i.e., we prove that if D is a K -central simple division algebra then $[D] \in U_F(K)$ if and only if D is K -isomorphic to what we call a uniform Kummer algebra, [see 4.1]. This classification yields a description of the division algebras underlying the cyclotomic algebras which represent the elements of $S(K)$, [20, Cor. 3.11, p. 33]. This is of particular interest when $S(K) = U(K)$. One of several examples we provide is an explicit description of the

quaternion division algebras over \mathbb{Q} in the form of a linearly independent generating set of division algebras for $U(\mathbb{Q})=S(\mathbb{Q})$. (By a linearly independent set $\{[D_i]\}$ in $B(K)$ we mean that whenever $\prod_i [D_i] \sim 1$ in $B(K)$ then $[D_i] \sim 1$ for each i in $B(K)$ where \sim denotes equivalence in $B(K)$.)

Let $S(K, \varphi)$ (respectively $U(K, \varphi)$) denote the subgroup of $S(K)$ consisting of all elements having $\text{ind}_{\mathfrak{p}} A = 1$ for all F -primes $\mathfrak{p} \neq \varphi$. Necessary and sufficient conditions for $S(K)$ to be the direct sum of $S(K, \varphi)$ as φ ranges over all F -primes are unknown. We present for the first time, necessary and sufficient conditions for $U_F(K)$ to be the direct sum of subgroups $U_F(K, \varphi)$ where φ ranges over all F -primes. From this result follows a new sufficient condition for $S(K)$ to be the direct product of the $S(K, \varphi)$. Moreover, several consequences of this result for $U_F(K)$ follow.

The author wishes to thank the National Research Council of Canada for their support of this research, and Steve Pierce for his moral support.

§1. Notation and Preliminaries

We will make full use of the following results concerning the power and norm residue symbols. The theory is well known and may be found for example in [2] or [5]. We state the results for algebraic number fields which are our major concern in this paper, but the theory holds in general for a given global field.

Let n be a fixed positive integer and K a fixed algebraic number field containing ε_n . Let S denote the set of K -primes containing the infinite primes and all primes dividing n . For elements $\alpha_i \in K^*$ let $S(\alpha_1, \dots, \alpha_r)$ denote the set of primes of S together with the K -primes dividing α_i for each i . Let I_K^S denote the subgroup of the ideal group I_K of K generated by the K -primes outside S . Now, for $\ell \in I_K^{S(\alpha)}$ the power residue symbol (α/ℓ) is defined by:

$$\sqrt[n]{\alpha^{\phi(\ell)}} = (\alpha/\ell) \sqrt[n]{\alpha}$$

where ϕ denotes the Artin map in $L = K(\sqrt[n]{\alpha})$ over K . We note that if \mathfrak{p} is a prime unramified in L then $\phi(\mathfrak{p})$ is the Frobenius automorphism of \mathfrak{p} . Moreover (α/ℓ) is an n^{th} root of unity independent of the choice of $\sqrt[n]{\alpha}$ and the following properties hold:

$$(1.1) \quad (\alpha \alpha' / \ell) = (\alpha/\ell)(\alpha'/\ell) \quad \text{if } \ell \in I^{S(\alpha, \alpha')}$$

$$(1.2) \quad (\alpha/\ell \ell') = (\alpha/\ell)(\alpha/\ell') \quad \text{if } \ell, \ell' \in I^{S(\alpha)}.$$

$$\text{Therefore: } (\alpha/\ell) = \prod_{\mathfrak{p} \notin S(\alpha)} (\alpha/\mathfrak{p})^{\alpha(\mathfrak{p})}$$

$$\text{where } \ell = \prod \mathfrak{p}^{\alpha(\mathfrak{p})}.$$

(1.3) (Generalized Euler Criterion). If $\mathfrak{p} \notin S(\alpha)$ then $N(\mathfrak{p}) \equiv 1 \pmod{n}$ where N denotes the norm in K/\mathbb{Q} , and (α/\mathfrak{p}) is the unique n^{th} root of unity such that $(\alpha/\mathfrak{p}) \equiv \alpha^{(N(\mathfrak{p})-1)/n} \pmod{\mathfrak{p}}$.

(1.4) For $\mathfrak{p} \notin S(\alpha)$ the following are equivalent

- (i) $(\alpha/\mathfrak{p}) = 1$.
- (ii) The congruence $x^n \equiv \alpha \pmod{\mathfrak{p}}$ is solvable with $x \in \mathcal{O}_{K_{\mathfrak{p}}}$.
- (iii) The equation $x^n = \alpha$ is solvable with $x \in K_{\mathfrak{p}}$.

(1.5) If \mathfrak{p} is an integral ideal prime to n then $(\zeta/\mathfrak{p}) = \zeta^{(N(\mathfrak{p})-1)/n}$ for $\zeta \in \langle \varepsilon_n \rangle$.

(1.6) If $\mathfrak{p} \in I^{S(\alpha, \alpha')}$ and

$$\alpha' \equiv \alpha \pmod{\mathfrak{p}}$$

then

$$(\alpha'/\mathfrak{p}) = (\alpha/\mathfrak{p}).$$

The following results concern the norm residue symbol and will be of particular interest throughout the paper.

For $\alpha, \beta \in K^*$ and an arbitrary prime \mathfrak{p} of K we define $(\alpha, \beta)_{\mathfrak{p}}$ by the equation:

$$(\sqrt[n]{\alpha})^{\psi_{\mathfrak{p}}(\beta)} = (\alpha, \beta)_{\mathfrak{p}} \sqrt[n]{\alpha}$$

where $\psi_{\mathfrak{p}}: K_{\mathfrak{p}}^* \rightarrow G(\mathfrak{p})$ is the local Artin map associated with $K(\sqrt[n]{\alpha})/K$, and $G(\mathfrak{p}) \simeq GK_{\mathfrak{p}}(\sqrt[n]{\alpha}/K_{\mathfrak{p}})$ is the decomposition group of \mathfrak{p} in $G(K(\sqrt[n]{\alpha})/K)$. Moreover, $(\alpha, \beta)_{\mathfrak{p}}$ is an n^{th} root of 1 which is independent of the choice of $\sqrt[n]{\alpha}$, and the following properties hold.

$$(1.7) \quad (\alpha, \beta)_{\mathfrak{p}}(\alpha, \beta')_{\mathfrak{p}} = (\alpha, \beta\beta')_{\mathfrak{p}}$$

and

$$(\alpha, \beta)_{\mathfrak{p}}(\alpha', \beta)_{\mathfrak{p}} = (\alpha\alpha', \beta)_{\mathfrak{p}}.$$

(1.8) If either α or $\beta \in (K_{\mathfrak{p}}^*)^n$ then $(\alpha, \beta)_{\mathfrak{p}} = 1$.

(1.9) If β is a norm from $K_{\mathfrak{p}}(\sqrt[n]{\alpha})$ then $(\alpha, \beta)_{\mathfrak{p}} = 1$.

$$(1.10) \quad (\alpha, \beta)_{\mathfrak{p}}(\beta, \alpha)_{\mathfrak{p}} = 1.$$

(1.11) If $\mathfrak{p} \notin S(\alpha)$ then $(\alpha, \beta)_{\mathfrak{p}} = \left(\frac{\alpha}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(\beta)}$ where $v_{\mathfrak{p}}$ denotes the \mathfrak{p} -adic valuation. In particular $(\alpha, \beta)_{\mathfrak{p}} = 1$ for $\mathfrak{p} \notin S(\alpha, \beta)$.

(1.12) For $\alpha, \beta \in K^*$ we have:

$$\prod (\alpha, \beta)_{\mathfrak{p}} = 1,$$

the product being taken over all the primes \mathfrak{p} of K .

Now we present some preliminary information concerning the Brauer groups and crossed products. The Schur subgroup $S(K)$ of the Brauer group $B(K)$ may be described as consisting of those equivalence classes which contain a simple component of the group algebra KG for some finite group G . By Yamada [20,

Cor. 3.11, p. 33] this is equivalent to $S(K)$ being the subgroup of $B(K)$ consisting of those equivalence classes which contain a cyclotomic algebra; i.e., a crossed product of the form $(K(\varepsilon), \gamma, \beta)$ where ε is a root of unity and the factor set β has values which are roots of unity in $K(\varepsilon)$.

In general we denote a crossed product by (L, G, β) which is the central simple K -algebra having L -basis u_τ , $\tau \in G = G(L/K)$ subject to:

$$u_{\tau, \alpha} = \beta(\tau, \alpha) u_{\tau\alpha}$$

and

$$u_\tau x = x^\tau u_\tau \quad \text{for } x \in L.$$

When G is cyclic then (L, γ, β) denotes the crossed product in which:

$$\begin{aligned} u_\tau^i &= u_{\tau^i} & 1 < i < |L:K| \\ &= \beta & \text{if } i = |L:K|. \end{aligned}$$

For further information on crossed products the reader is referred to the beautifully written book by Reiner [17]. Note also that most fundamental results concerning the Schur group may be found in [20].

Finally we give some comments on notation. When we write a tensor product $D \otimes K$ we assume this tensor product is taken over the centre of the factor on the left.

§2

In the case where p is an odd rational prime and K/Q is finite abelian, Janusz [7, §6, p. 276] has mentioned certain sufficient conditions for $S(K)_p$ to be the direct sum of groups $S(K, q)$ as q ranges over all rational primes. However necessary and sufficient conditions are unknown. The first result of this section allows us to present a new sufficient condition for this to occur in the more general case where K/F is a finite Galois extension of number fields, while solving the problem for $U_F(K)$.

We now set the stage for the theorem. We let $G = G(K/F)$, and for a given F -prime φ the decomposition group of a K -prime $\hat{\varphi}$ above φ , in G is denoted by $G(\hat{\varphi})$. The rational prime which φ divides is denoted by q .

We now present for the first time necessary and sufficient conditions for $U_F(K)$ to be the direct sum of groups $U_F(K, \varphi)$ as φ ranges over all F -primes.

Theorem 2.1. *There exists*

$$[A] \in U_F(K, \varphi)$$

with $\text{ind}_\varphi A = n$ if and only if

- (1) ε_n is in K , and

(2) $\sum b_j^{-1} \equiv 0 \pmod{n}$ where $\varepsilon_n^{\sigma_j} = \varepsilon_n^{b_j}$ for coset representatives σ_j of $G(\hat{\varphi})$ in G with $\hat{\varphi}$ any K -prime above φ and b_j^{-1} the multiplicative inverse of b_j modulo n ; $0 < b_j < n$.

Proof. Assume $[A] \in U_F(K, \varphi)$ with $\text{ind}_\varphi A = n$. By the definition of $U_F(K)$, ε_n is in K .

For the remainder of the theorem we let $\hat{\varphi}_j$; $j=1, 2, \dots, g$ be the distinct K -primes above φ with $\hat{\varphi}_1 = \hat{\varphi}$. We may assume $\hat{\varphi}_1^{\sigma_j} = \hat{\varphi}_j$ for $j=1, 2, \dots, g$ where $\{\sigma_j\}$ are as in (2) above; see [5, §5.4, pp. 82–84]. By Mollin [13, Corollary 2.6, p. 255] we may assume $\text{inv}_{\hat{\varphi}_j} A = 1/n$, and so it follows that:

$$\text{inv}_{\hat{\varphi}_j} A \equiv b_j^{-1} \text{inv}_{\hat{\varphi}_j} A \equiv b_j^{-1}/n \pmod{1}.$$

Hence: $\sum_j \text{inv}_{\hat{\varphi}_j} A \equiv \sum_j b_j^{-1}/n \pmod{1}$. Since $\text{ind}_{\hat{\varphi}_j} A = 1$ for all F -primes $\hat{\varphi}_j \neq \varphi$ then by Hasse's sum theorem we get $\sum_j b_j^{-1} \equiv 0 \pmod{n}$ as required.

Conversely assume (1) and (2). Define a central simple K -algebra A by

$$\text{inv}_{\hat{\varphi}} A = 1/n \quad \text{and} \quad \text{inv}_{\hat{\varphi}_j} A = b_j^{-1}/n$$

and $\text{inv}_{\hat{\varphi}_j} A = 0$ for all K -primes $\hat{\varphi}_j$ not dividing φ . Thus $\sum_j \text{inv}_{\hat{\varphi}_j} A = \sum_j (b_j^{-1}/n) \equiv 0 \pmod{1}$ by (2), and so by Hasse's sum theorem $[A]$ exists in $B(K)$. By (1) and the construction of A we have in fact that $[A] \in U_F(K, \varphi)$ with $\text{ind}_\varphi A = n$. Q.E.D.

Now, let m be the order of the group of roots of unity in K . In the following corollary we assume $\mathbb{Q}(\varepsilon_m) \cap F = \mathbb{Q}$.

Corollary 2.2. *There exists $[A] \in U_F(K, \varphi)$ with $\text{ind}_\varphi A = n > 2$ for $\varphi \nmid n$ if and only if ε_n is in K and $q^f \equiv 1 \pmod{n}$ where f is the residue class degree of φ in F/\mathbb{Q} .*

Proof. Since $\varphi \nmid n$ then φ is completely split in $F(\varepsilon_n)/F$ if and only if $q^f \equiv 1 \pmod{n}$. Now we show that there exists $[A] \in U_F(K, \varphi)$ with $\text{ind}_\varphi A = n$ if and only if φ is completely split in $F(\varepsilon_n)/F$.

By Mollin [13, Th. 2.3, p. 251], if $[A] \in U_F(K)$ with $\text{ind}_\varphi A = n$ then φ splits in $F(\varepsilon_n)/F$. Conversely if ε_n is in K and φ is completely split in $F(\varepsilon_n)/F$ then choose coset representatives $\{\sigma_j\}$ of $G(\hat{\varphi})$ in G through $H = G(K/F(\varepsilon_n))$ where $\hat{\varphi}$ is a K -prime above φ . Now if $\varepsilon_n^{\sigma_j} = \varepsilon_n^{b_j}$ then

$$\sum b_j^{-1} = |H : D(\hat{\varphi})| \sum_{j=1}^{\phi(n)} t_j$$

where $0 < t_j < n$; $(t_j, n) = 1$ and ϕ is the Euler function. Since $\mathbb{Q}(\varepsilon_m) \cap F = \mathbb{Q}$ and ε_n is in K then $n|m$; so $G(F(\varepsilon_n)/F)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$ and since $n > 2$ then $\phi(n) > 1$. Hence the t_j may be arranged in pairs $t_j, n - t_j$ which implies $\sum b_j^{-1} \equiv 0 \pmod{n}$. By Theorem 2.1 there exists $[A] \in U_F(K, \varphi)$ with $\text{ind}_\varphi A = n$. This secures the theorem. Q.E.D.

We note that the above corollary generalizes [13, Th. 2.7, p. 256], [9, Th. 1.5, p. 274] and [9, Th. 1.1, p. 273]. The latter generalized Witt's results [19,

Th.10.11, p.243]) for K/\mathbb{Q} finite abelian. Thus we have pushed the generalization to the case where K/F is finite Galois under the hypothesis of Corollary 2.2.

Furthermore for $F=\mathbb{Q}$ we note that by examining the proof of Corollary 2.2 we get the following corollary as an immediate consequence there of.

Corollary 2.3. *If p is an odd prime and K/\mathbb{Q} is finite Galois then $U(K)_p$ is the direct sum of groups $U(K, q)_p$ as q ranges over all rational primes.*

Corollary 2.4. *If p is an odd prime, ε_{p^a} is the highest p -power root of unity in K , where K/\mathbb{Q} is finite abelian and $p \nmid |K:\mathbb{Q}(\varepsilon_{p^a})|$ then $S(K)_p$ is the direct sum of $S(K, q)_p$ as q ranges over all rational primes.*

Proof. From Mollin [9, Corollary 2.8, p.280] $U(K)_p = S(K)_p$. The result is now immediate from Corollary 2.3. Q.E.D.

§3

The following results from Kummer theory will be useful in establishing the main theorem of this section.

Lemma 3.1. *The discriminant of $L=K(\sqrt[n]{\alpha})$ over K divides $n^n \alpha^{n-1}$ and q is unramified in L/K if q does not divide $\mathcal{O}_K \cdot n\alpha$. Thus if α^f is the least power of α such that $\alpha^f \equiv x^n \pmod{q}$ is solvable then f is the residue class degree of q in L/K .*

Proof. See [2, Lemma 5, p.91].

Lemma 3.2. *Let p be a rational prime and assume ε_p is in K .*

Let $L=K(\sqrt[p]{\alpha})$ where α is not a p^{th} power of an element of K . Let $\mathfrak{p}|\mathcal{O}_K \cdot p$; $\mathfrak{p} \nmid \alpha$ and $\mathcal{O}_K(1-\varepsilon_p) = \mathfrak{p}^m \cdot J$ where \mathfrak{p} and J are relatively prime then:

If the congruence $x^p \equiv \alpha \pmod{\mathfrak{p}^{mp}}$ has no solution in \mathcal{O}_K then \mathfrak{p} is ramified in L .

If $x^p \equiv \alpha \pmod{\mathfrak{p}^{mp+1}}$ is solvable in \mathcal{O}_K then \mathfrak{p} splits in L . Finally, if $x^p \equiv \alpha \pmod{\mathfrak{p}^{mp}}$ is solvable in \mathcal{O}_K but the above congruence is not, then \mathfrak{p} is inert in L .

Proof. Ribenoim [18, 6C, p.278].

The following existence theorem will be crucial in proving the main result of the next section.

Theorem 3.3. *Let K be a finite Galois extension of \mathbb{Q} with ε_n in K where $n=p^d$, $d>0$, p being a rational prime. Let $S=\{q_i\}$ be a finite set of distinct rational primes with q_i completely split in $\mathbb{Q}(\varepsilon_n)/\mathbb{Q}$.*

Let φ_i be a fixed K -prime above q_i and denote by $\{\sigma_1^{(i)}, \sigma_2^{(i)}, \dots, \sigma_g^{(i)}\}$ distinct coset representatives of $G(\varphi_i)$, the decomposition group of φ_i in $G=G(K/\mathbb{Q})$ with $\varepsilon_n^{\sigma_j^{(i)}} = \varepsilon_n^{b_j^{(i)}}$; g.c.d. $(b_j^{(i)}, n)=1$. Suppose that $\sum_{i,j} [b_j^{(i)}]^{-1} \equiv 0 \pmod{n}$. Then there exists α , $\beta \in \mathcal{O}_K$, the ring of integers of K , such that:

$$(1) \quad (\beta) = \mathfrak{a} = \prod_{i,j} (\varphi_i^{\sigma_j^{(i)}})^{[b_j^{(i)}]^{-2}}$$

where φ_i are finite and \mathfrak{s} is a K -prime which is relatively prime to $\varphi_i^{\sigma_i^{(i)}}$ for all i, j and to \mathfrak{p} for all K -primes \mathfrak{p} above p . Moreover, if φ_i is (real) infinite then $\beta_{\varphi_i}^{\sigma_i^{(i)}} < 0$ for all j ; (where $\beta_{\mathfrak{p}}$ is the image of β under the map $K \rightarrow K_{\mathfrak{p}}$).

(2) $(\alpha) = \mathfrak{z}$, a K -prime which is relatively prime to \mathfrak{s} , all K -primes \mathfrak{p} above p , and to the (finite) $\varphi_i^{\sigma_i^{(i)}}$.

$$(3) (\alpha, \beta)_{\mathfrak{s}} = 1.$$

(4) For each $\mathfrak{p} | p$ with $\mathfrak{p} \neq \varphi_i^{\sigma_i^{(i)}}$ then $(\alpha, \beta)_{\mathfrak{p}} = 1$.

(5) $(\alpha, \beta)_{\varphi_i} = \varepsilon_n = (\alpha^{[\sigma_i^{(i)}]^{-1}}, \beta)_{\varphi_i}$, for all i, j where φ_i is finite.

$$(6) (\alpha, \beta)_{\mathfrak{s}} = 1.$$

Proof. Let $\mathcal{A} = \prod_{i,j} (\varphi_i^{\sigma_i^{(i)}})^{(b_j^{(i)})^{-2}}$ and let $\overline{\mathcal{A}}$ denote the class of \mathcal{A} in the class group of K , (respectively the extended class group of \overline{K} whenever there are infinite primes in S ; [8, § 3, p. 203]). Choose a prime $\mathfrak{s} \in \overline{\mathcal{A}}^{-1}$ such that \mathfrak{s} is relatively prime to \mathcal{A} and to \mathfrak{p} for each $\mathfrak{p} | p$. This choice is allowed by [8, 10.3, p. 182; 4.6.2, p. 132]. Thus $\mathfrak{s}\mathcal{A} = (\beta)$ where $\beta \in \mathcal{O}_K$. If infinite primes exist in S then we choose $-\beta$ rather than β . In this case β is totally positive since we considered the extended class group. Hence the image of $-\beta$ in $K_{\mathfrak{p}}$ is negative for the real infinite prime $\mathfrak{p} \in S$. We now have (1).

Since \mathfrak{s} , the \mathfrak{p} 's and the $\varphi_i^{\sigma_i^{(i)}}$'s are relatively prime then by [17, 4.11, p. 48] there exists a solution γ to the following congruences: $x \equiv 1 \pmod{\mathfrak{s}}$; $x \equiv a^{\sigma_i^{(i)}} \pmod{\varphi_i^{\sigma_i^{(i)}}}$ for all $\varphi_i^{\sigma_i^{(i)}} \nmid p$ where $a \in K$ is a p^{d-d_i} -th power modulo φ_i but not a p^{d-d_i+1} -th power modulo φ_i ; (the existence of a is guaranteed by the fact that φ_i being completely split in $Q(\varepsilon_n)/Q$ implies $\varphi_i \equiv 1 \pmod{n_i}$), and for

$$\mathfrak{p} | p, \quad \mathfrak{p} \neq \varphi_i^{\sigma_i^{(i)}} \quad \text{for all } i, j;$$

$x \equiv 0 \pmod{\mathfrak{p}^{m_p+1}}$. We note that if $\mathfrak{p} | p$ and $\mathfrak{p} \in S$ then by hypothesis p is completely split in $Q(\varepsilon_n)/Q$. Thus $p^d = n = 2$. For such \mathfrak{p} , $x \equiv b^{\sigma_i^{(i)}} \pmod{[\mathfrak{p}^{\sigma_i^{(i)}}]^{m_p}}$ with b being a square modulo \mathfrak{p}^{m_p} but not a square modulo \mathfrak{p}^{m_p+1} .

Now choose a prime \mathfrak{z} in the class $\overline{(\gamma)}$ such that \mathfrak{z} is relatively prime to the \mathfrak{p} 's, the $\varphi_i^{\sigma_i^{(i)}}$'s and to \mathfrak{s} . Then $\mathfrak{z} = (\alpha)$, and we have (2).

Since $\alpha \equiv 1 \pmod{\mathfrak{s}}$ then $(\alpha, \beta)_{\mathfrak{s}} = 1$ which is (3). For each $\mathfrak{p} | p$ with $\mathfrak{p} \neq \varphi_i^{\sigma_i^{(i)}}$ then $\alpha \equiv 0 \pmod{\mathfrak{p}^{mn+n}}$ yields from Lemma 3.2 that $(\alpha, \beta)_{\mathfrak{p}} = 1$, which is (4). If $\mathfrak{p} | p$ and $\mathfrak{p} = \varphi_i^{\sigma_i^{(i)}}$ then $\alpha \equiv b^{\sigma_i^{(i)}} \pmod{[\mathfrak{p}^{\sigma_i^{(i)}}]^{mn}}$ yields $\alpha^{[\sigma_i^{(i)}]^{-1}} \equiv b \pmod{\mathfrak{p}^{mn}}$. By Lemma 3.2 the choice of b guarantees:

$$(\alpha^{[\sigma_i^{(i)}]^{-1}}, \beta)_{\varphi_i} = (\alpha, \beta)_{\varphi_i}^{\sigma_i^{(i)}} = \varepsilon_n.$$

Now for $\varphi_i^{\sigma_i^{(i)}} \nmid p$ then $\alpha \equiv a^{\sigma_i^{(i)}} \pmod{\varphi_i^{\sigma_i^{(i)}}}$. Thus from (1.3) $(\alpha^{[\sigma_i^{(i)}]^{-1}}/\varphi_i) = (\alpha/\varphi_i) = \varepsilon_n$ by Lemma 3.1. By the choice of β we have $v_{\varphi_i}(\beta) = 1$ for all i , so from (1.11),

$$(\alpha, \beta)_{\varphi_i} = (\alpha/\varphi_i) = (\alpha^{[\sigma_i^{(i)}]^{-1}}/\varphi_i) = (\alpha^{[\sigma_i^{(i)}]^{-1}}, \beta)_{\varphi_i} = \varepsilon_n$$

for all i, j . This is (5).

Now extend each $\sigma_j^{(i)}$ to $G(\bar{L}/F)$ such that $\sqrt[n]{\alpha^{\sigma_j^{(i)}}} = \sqrt[n]{\alpha^{\sigma_j^{(i)}}}$, where \bar{L} is the normal closure of $L = K(\sqrt[n]{\alpha})$ over F , and we maintain σ_j as notation for the extended automorphism. From [8, 2.2–2.4, pp. 98–99] the fact that $\varphi_i^{\sigma_j^{(i)}}$ is unramified in L guarantees $[\sigma_j^{(i)}]^{-1} \psi_{\varphi_i}(\beta) \sigma_j^{(i)} = \psi_{\varphi_i^{\sigma_j^{(i)}}}(\beta)$ where ψ_{φ} is the local Artin map. Therefore:

$$(\alpha^{[\sigma_j^{(i)}]^{-1}}, \beta)_{\varphi_i^{\sigma_j^{(i)}}} = (\alpha, \beta)_{\varphi_i^{\sigma_j^{(i)}}}.$$

But

$$(\alpha^{[\sigma_j^{(i)}]^{-1}}, \beta)_{\varphi_i} = (\alpha, \beta)_{\varphi_i}.$$

Therefore

$$\begin{aligned} \prod_{i,j} (\alpha, \beta)_{\varphi_i^{\sigma_j^{(i)}}} &= \prod_{i,j} (\alpha, \beta)_{\varphi_i^{\sigma_j^{(i)}}} \\ &= \prod_{i,j} \varepsilon_n^{\sigma_j^{(i)}} = \varepsilon_n^{\sum b_j^{(i)}} = 1 \end{aligned}$$

by hypothesis. Hence we have:

$$\prod_{\tau \neq \hat{\sigma}} (\alpha, \beta)_{\tau} = 1.$$

By the product formula we must have $(\alpha, \beta)_{\hat{\sigma}} = 1$ which is (6). Q.E.D.

§ 4. Uniform Kummer Algebras

Throughout this section K/Q will denote a finite Galois extension of number fields with ε_n in K . A *Kummer algebra* over K is a crossed product $(L/K, \sigma, \beta)$ where $G(L/K)$ is of exponent n and the values of β are algebraic integers in L .

We note that the fundamental theorem of Kummer theory asserts that L/K is a Kummer extension; i.e., $L = K(\sqrt[n]{\alpha_1}, \dots, \sqrt[n]{\alpha_r})$ where $\{\alpha_1, \dots, \alpha_r\}$ is a system of coset representatives of $M_L = \{y \in K : y = x^n, x \in L^*\}$ over K^n and $|L:K| = |M_L : K^{*n}|$. For details the reader is referred to [8, § 8].

By studying such algebras Hasse provided a clear link-up of norm residues with his generalization of the Hilbert symbol. In fact he did not require the existence of n^{th} roots of unity in K , (see [6]).

Also by investigating these algebras Chevalley was the first to define a local Artin symbol in the ramified case, (see [3]–[4]).

These connections provide class field-theoretic methods of dealing with our classification problem.

We shall be interested in special kinds of Kummer algebras which we now introduce.

Definition 4.1. A *Uniform Kummer Algebra* of index n over K relative to F is a cyclic Kummer division algebra D such that whenever $D \otimes_{K_{\hat{\sigma}}} K_{\hat{\sigma}} \sim 1$ for some K -prime $\hat{\sigma}$ then $D \sim (K(\sqrt[n]{\alpha}), \gamma, \beta)$ where

- (1) $\hat{\sigma}$ is unramified in $K(\sqrt[n]{\alpha})$, for $\hat{\sigma}$ finite

(2) Suppose $|K_{\hat{\varphi}}(\sqrt[m]{\alpha}):K_{\hat{\varphi}}|=m$, and $\{\sigma_j\}$ is a set of coset representatives of $G(\hat{\varphi})$ the decomposition group of $\hat{\varphi}$ in $G(K/F)$ with $e_m^{\sigma_j} = e_m^{b_j}$; $\text{g.c.d.}(b_j, m) = 1, 0 < b_j < m$. Then

$$(\alpha^{\sigma_j^{-1}}, \beta)_{\hat{\varphi}} = (\alpha, \beta)_{\hat{\varphi}} = \varepsilon_m \quad \text{and} \quad v_{\hat{\varphi}}(\beta) = b_j^{-2} v_{\hat{\varphi}}^{\sigma_j}(\beta) \pmod{m}$$

for all j .

Now we are in a position to prove the main result.

Theorem 4.2. *Let D be a K -central simple division algebra. Then $[D] \in U(K)$ if and only if D is K -isomorphic to a Uniform Kummer algebra over K relative to Q .*

Proof. Let $D = (K(\sqrt[m]{\alpha}), \gamma, \beta)$ be a Uniform Kummer algebra over K relative to Q , with $D \otimes K_{\hat{\varphi}} \sim 1$. Let $\{\sigma_j\}$ be coset representatives of $G(\hat{\varphi})$ in $G = G(K/Q)$. By Definition 4.1, finite $\hat{\varphi}$ is unramified in $K(\sqrt[m]{\alpha})$ and $(\alpha, \beta)_{\hat{\varphi}} = \varepsilon_m$, where $m = |K_{\hat{\varphi}}(\sqrt[m]{\alpha}):K_{\hat{\varphi}}|$. Therefore, by [2, Prop. 2, p. 141; Prop. 1.2, p. 163] we get $\psi_{\hat{\varphi}}(\beta) = \mathcal{F}(\hat{\varphi})$ where $\psi_{\hat{\varphi}}$ is the local Artin map and $\mathcal{F}(\hat{\varphi})$ is the Frobenius automorphism of $\hat{\varphi}$ in $\hat{G} = G(L/K)$ where $L = K(\sqrt[m]{\alpha})$. Now we extend each σ_j to $G(\bar{L}/Q)$ such that $\sqrt[m]{\alpha^{\sigma_j}} = \sqrt[m]{\alpha^{\sigma_j}}$, where \bar{L} is the normal closure of L over Q , and we maintain σ_j as notation for the extended automorphism. From [8, 2.2–2.4, pp. 98–99] we get $\sigma_j^{-1} \psi_{\hat{\varphi}}(\beta) \sigma_j = \psi_{\hat{\varphi}^{\sigma_j}}(\beta)$. Also since $(\alpha^{\sigma_j^{-1}}, \beta)_{\hat{\varphi}} = (\alpha, \beta)_{\hat{\varphi}} = \varepsilon_m$ and $e_m^{\sigma_j} = e_m^{b_j}$ then $\psi_{\hat{\varphi}^{\sigma_j}}(\beta) = \psi_{\hat{\varphi}}(\beta)^{b_j}$. Therefore

$$\mathcal{F}(\hat{\varphi}^{\sigma_j}) = \mathcal{F}(\hat{\varphi})^{b_j}. \tag{*}$$

Let k be the least positive integer such that $\gamma^k \in \hat{G}(\hat{\varphi})$, the decomposition group of $\hat{\varphi}$ in \hat{G} . Then $D \otimes K_{\hat{\varphi}} \sim (K_{\hat{\varphi}}(\sqrt[m]{\alpha}), \gamma^k, \beta)$, and if r is an integer relatively prime to $|\hat{G}(\hat{\varphi})|$ with $\gamma^{kr} = \mathcal{F}(\hat{\varphi})$ then $\text{inv}_{\hat{\varphi}} D = r v_{\hat{\varphi}}(\beta)/m$, (see [17, p. 281]). From (*) it follows that k is the least positive integer such that $\gamma^k \in \hat{G}(\hat{\varphi}^{\sigma_j})$ and that $\gamma^{kr b_j} = \mathcal{F}(\hat{\varphi}^{\sigma_j})$. Therefore: $D \otimes K_{\hat{\varphi}^{\sigma_j}} \sim (K_{\hat{\varphi}^{\sigma_j}}(\sqrt[m]{\alpha}), \gamma^k, \beta)$ with $\text{inv}_{\hat{\varphi}^{\sigma_j}} D = b_j v_{\hat{\varphi}^{\sigma_j}}(\beta) \cdot r/m$. By Definition 4.1 we have:

$$\begin{aligned} \text{inv}_{\hat{\varphi}^{\sigma_j}} D &\equiv b_j \cdot b_j^{-2} v_{\hat{\varphi}}(\beta) \cdot r/m \pmod{1} \\ &\equiv b_j^{-1} \text{inv}_{\hat{\varphi}} D \pmod{1}. \end{aligned}$$

From definition 4.1 if $\hat{\varphi} = \infty$ then $\text{inv}_{\hat{\varphi}^{\sigma_j}} D = \text{inv}_{\hat{\varphi}} D$. Hence $[D] \in U_F(K)$ as required.

It suffices to prove the converse for $[D] \in U(K)_p$ where D has index $n = p^d$, p a rational prime, where D is a generator. Thus for $\{\varphi_1, \dots, \varphi_g\}$ the distinct F -primes where $1 < \text{ind}_{\varphi_i} D = n$. Now for each i choose and fix a K -prime $\hat{\varphi}_i$ above φ_i such that $\text{inv}_{\hat{\varphi}_i} A = 1/n$, (see [13, Cor. 2.6, p. 255]).

Let $\{\sigma_j^{(i)}\}$ be distinct coset representative of $G(\hat{\varphi}_i)$ in G with $e_n^{\sigma_j^{(i)}} = e_n^{b_j^{(i)}}$, $\text{g.c.d.}(b_j^{(i)}, n) = 1$. We have that since $[D] \in U(K)_p$:

$$\text{inv}_{\hat{\varphi}_i^{\sigma_j^{(i)}}} D \equiv [b_j^{(i)}]^{-1} \text{inv}_{\hat{\varphi}_i} D \equiv [b_j^{(i)}]^{-1}/n \pmod{1}.$$

Hence:

$$\sum_{i,j} \text{inv}_{\hat{\varphi}_i^{\sigma_j^{(i)}}} D \equiv \sum_{i,j} [b_j^{(i)}]^{-1}/n \equiv 0 \pmod{1},$$

by Hasse's sum theorem.

So:

$$\sum_{i,j} [b_j^{(i)}]^{-1} \equiv 0 \pmod{n}.$$

Moreover by Mollin [13, Th. 2.3, p. 251] φ_i is completely split in $Q(\varepsilon_n)/Q$ for all i . Therefore the hypothesis of Theorem 3.3 is satisfied, so we may choose $\alpha, \beta \in \mathcal{O}_K$ satisfying (1)–(6) of Theorem 3.3.

Set $D_1 = (K(\sqrt[n]{\alpha}), \gamma, \beta)$. From Theorem 3.3, D_1 is a Uniform Kummer algebra over K relative to Q . We now show $D \sim D_1$.

Let k_i be the smallest positive integer such that $\gamma^{k_i} \in \hat{G}(\hat{\varphi}_i)$. Since $\hat{\varphi}_1$ is unramified in $K(\sqrt[n]{\alpha})$ and $|K_{\hat{\varphi}_1}(\sqrt[n]{\alpha}) : K_{\hat{\varphi}_1}| = n$ then we may assume without loss of generality that $\gamma = \mathcal{F}(\hat{\varphi}_1)$.

Since $D_1 \otimes K_\tau \sim 1$ if and only if $(\alpha, \beta)_\tau = 1$, [1, Th. 7, p. 95] then by Theorem 3.3, $D \otimes K_\tau \sim 1$ for all $\tau \neq \hat{\varphi}_i^{\sigma(i)}$. Consider, for each i , $D_1 \otimes K_{\hat{\varphi}_i} \sim (K_{\hat{\varphi}_i}(\sqrt[n]{\alpha}), \gamma^{k_i}, \beta)$. Then $\text{inv}_{\hat{\varphi}_i} D_1 = v_{\hat{\varphi}_i}(\beta)/n$, (see [17, p. 281]). But, by Theorem 3.3, $v_{\hat{\varphi}_i}(\beta) = 1$ so $\text{inv}_{\hat{\varphi}_i} D_1 = \text{inv}_{\hat{\varphi}_i} D$ for each i . From Mollin [13, Lemma 2.9, p. 259] it follows that $D_1 \sim D$ as required. Q.E.D.

§ 5. Examples

First we exhibit the quaternion division algebras over \mathbb{Q} as uniform Kummer algebras. Since $U(\mathbb{Q}) = S(\mathbb{Q})$, [20, Th. 7.2, p. 96] then the following gives a description of the division algebras underlying the cyclotomic algebras which represent the elements of $S(\mathbb{Q})$.

For rational primes $p \neq 2$ choose a prime $q_p \equiv 3 \pmod{4}$ such that $(q_p/p) = (-1)^{(p+1)/2}$, and if $p = 2$ choose $q_2 \equiv 3 \pmod{8}$. Set $D_{p,\infty} = (\mathbb{Q}(\sqrt{-q_p}), \gamma, -p)$, where ∞ denotes the infinite rational prime. It is easily seen that $D_{p,\infty}$ is a Kummer algebra. We now show that in fact $D_{p,\infty}$ is a Uniform Kummer algebra and $\{D_{p,\infty}\}_p$ where p ranges over all finite rational primes forms an independent set of division algebras which represent the classes of $U(\mathbb{Q}) = S(\mathbb{Q})$. First we calculate the Hasse invariants of $D_{p,\infty}$. As previously cited $D_{p,\infty} \otimes \mathbb{Q}_\tau \sim 1$ if and only if $(-q_p, -p)_\tau = 1$. Now, since $(-q_p, -p)_\tau = 1$ for all $\tau \neq q_p, p, \infty$; [8, Prop. 3.11, p. 153] then $D_{p,\infty} \otimes \mathbb{Q}_\tau \sim 1$ for all $\tau \neq q_p, p, \infty$. We check for the remaining primes.

$$\begin{aligned} (-q_p, -p)_\infty &= -1, \\ (-q_p, -p)_p &= (-1, p)_p (q_p, p)_p (-1, -1)_p (q_p, -1)_p \quad \text{by (1.7)} \\ &= \begin{cases} (1) (-1) (1) (1) & \text{for } p \equiv 1 \pmod{4} \\ (-1) (1) (1) (1) & \text{for } p \equiv 3 \pmod{4} \\ (1) (-1) (-1) (-1) & \text{for } p = 2. \end{cases} \\ &= -1 \quad \text{for any finite } p. \\ (-q_p, -p)_{q_p} &= (-p/q_p) = (-1/q_p)(p/q_p) = -(p/q_p) = 1 \quad \text{by (1.1)–(1.11).} \end{aligned}$$

Hence $D_{p,\infty}$ has non-trivial Hasse invariants exactly at p , and ∞ . But the index of $D_{p,\infty}$ must divide $|\mathbb{Q}(\sqrt{-q_p}) : \mathbb{Q}| = 2$. Therefore $\text{inv}_p D_{p,\infty} = \text{inv}_{p,\infty} D_{p,\infty} = 1/2$. From the above we see that $D_{p,\infty}$ is a uniform Kummer algebra and $\{D_{p,\infty}\}_p$ clearly forms an independent set of division algebra representatives of $U(\mathbb{Q}) = S(\mathbb{Q})$.

Now let $K = \mathbb{Q}(\sqrt{d})$ where $d \neq -1$ is a square-free integer. In Mollin [12] we gave an explicit description of cyclic crossed product division algebras which generate $U(\mathbb{Q}(\sqrt{d}))$. The only distinction between those algebras $A = (K(\sqrt{\beta}), \gamma, \alpha)$ and the uniform Kummer algebras of Definition 4.1 is that $A \otimes K_q \sim 1$ for q ramified in $K(\sqrt{\beta})/K$. However, from the property of the norm residue symbol: $(\alpha, \beta)_q (\beta, \alpha)_q = 1$ it follows that $A \sim (K(\sqrt{\alpha}), \gamma', \beta)$. Hence from [12] we essentially have a description of all uniform Kummer algebras over $\mathbb{Q}(\sqrt{d}) = K$.

The next example provides a description of the Uniform Kummer algebras which represent the classes of $U(\mathbb{Q}(\epsilon_3))_3 = S(\mathbb{Q}(\epsilon_3))_3$ (see Mollin [9, Cor. 2.8, p. 820]). First we need a lemma.

Lemma 5.1. *Given an odd prime p and a prime $q \equiv 1 \pmod{p}$ there exists a prime r such that q is a p^{th} power modulo r but r is not a p^{th} -power modulo q .*

Proof. By the Chinese remainder theorem there is a solution to (1) $x \equiv 2 \pmod{p}$ and (2) $x \equiv g \pmod{q}$ where g is a primitive root modulo q . By Dirichlet's theorem on primes in arithmetic progression we may choose a prime r from $\{a + pqn\}_{n \in \mathbb{Z}}$ where a is a solution of (1) and (2).

We now show that (1) guarantees that q is a p^{th} power modulo r . Let h be a primitive root modulo r , and suppose $q \equiv h^v \pmod{r}$. Since $\text{g.c.d.}(r-1, p) = 1$ then for suitable s and t the following congruence is solvable: $h^{pt - (r-1)s} \equiv h^v \pmod{r}$. Hence, q is a p^{th} -power modulo r .

Since $q \equiv 1 \pmod{p}$ and g is a primitive root modulo q then (2) yields that r is not a p^{th} power modulo q . Q.E.D.

Let $K = \mathbb{Q}(\epsilon_3)$, $F = \mathbb{Q}$ and $q \equiv 1 \pmod{3}$. Set $D_q = (\mathbb{Q}(\epsilon_3, \sqrt[3]{r}), \gamma, q)$ where r is a prime chosen as in Lemma 5.1. We now show that the division algebras D_q provide an independent set of representatives of the generator classes in $U_F(K)_3 = S(K)_3$.

Since a unit is a norm in an unramified extension, [8, Prop. 3.11, p. 153] then $(r, q)_\tau = 1$ for all K -primes $\tau \neq \rho, \nu, \rho_1, \rho_2$ where $\rho \nmid 3$, $\nu | r$, and $\rho_i | q$. Thus $D_q \otimes K_\tau \sim 1$ for all K -primes $\tau \neq \rho, \nu, \rho_1, \rho_2$ by [1, Th. 7, p. 95].

Now we check for the remaining primes. Since q is a cube modulo r then q is a cube modulo ν . Therefore by (1.11), $1 = (q/\nu) = (q, r)_\nu$. Thus $D_q \otimes \mathbb{Q}_\nu(\epsilon_3) \sim 1$.

Since r is not a cube modulo q , and $\mathbb{Q}_q(\epsilon_3) = \mathbb{Q}_q$ since $q \equiv 1 \pmod{3}$ then we may assume without loss of generality that $(r/q) = \epsilon_3$. Also if $\langle \theta \rangle = G(K/\mathbb{Q})$ then $(r/q_1^\theta) = (r/q_1)^\theta = \epsilon_3^2$. Hence

$$\text{inv}_{\rho_1} D_q = 1/3 \quad \text{and} \quad \text{inv}_{\rho_2} D_q = 2/3.$$

The only prime which we have not checked is $\rho \nmid 3$. By the product formula $(r, q)_\rho = 1$ is forced. We have shown that D_q is a uniform Kummer algebra with

$\text{ind}_q D_q = 3$ and $\text{ind}_s D_q = 1$ for all rational prime $s \neq q$. These are the generators of $U(\mathbb{Q}(\varepsilon_3))_3 = S(\mathbb{Q}(\varepsilon_3))_3$ as division algebras.

As a final example we illustrate a connection between the main result of §4 and a sufficient condition given in Mollin [13] for the existence of an element in $U_F(K)$.

Let $K = \mathbb{Q}(\varepsilon_{2^{n+1}}, \sqrt{q})$ where $n \geq 2$, and $q \equiv 3 \pmod{2^{n+1}}$. Let $D = (K(\varepsilon_{2^{n+2}}), \gamma, \sqrt{q})$. We show that $[D] \in U(K)$ and that D is a Uniform Kummer algebra. Since the order of $q \pmod{2^{n+1}}$ is 2^{n-1} and $q^{2^{n-1}} \not\equiv 1 \pmod{2^{n+2}}$ then:

$$(\varepsilon_{2^{n+1}}, \sqrt{q})_\varphi = (\varepsilon_{2^{n+1}}/\varphi) \equiv \varepsilon_{2^{n+1}}^{(q^{2^{n-1}} - 1)/2} \equiv -1 \pmod{\varphi}$$

for each K -prime φ above q . Thus $\text{inv}_\varphi D = 1/2$ for all K -primes φ above q . Since there is only one K -prime above 2 and $D \otimes K_\tau \sim 1$ for all K -primes τ not above q or 2 then the product formula forces $\text{inv}_\tau D = 0$ for all K -primes τ not above q . By construction D is a uniform Kummer algebra and so $[D] \in U(K)$.

It is interesting to note that since $(\varepsilon_{2^{n+1}}, \sqrt{q})_\varphi (\sqrt{q}, \varepsilon_{2^{n+1}})_\varphi = 1$

then

$$D \sim (\mathbb{Q}(\varepsilon_{2^{n+1}}, \sqrt[4]{q}), \gamma', \varepsilon_{2^{n+1}}) = D_1.$$

Set $L = \mathbb{Q}(\varepsilon_{2^{n+1}}, \sqrt[4]{q})$. $G(L|\mathbb{Q})$ is the direct product of the cyclic group of order 2, the cyclic group of order 2^{n-2} , and the Dihedral group of order 8. Moreover $G(L/K)$ is central in $G(L/\mathbb{Q})$. This latter condition on D_1 was a sufficient condition for a crossed product algebra (not necessarily a division algebra) to lie in $U_F(K)$, (see Mollin [13]).

A question pertaining to $S(K)$ and uniform Kummer algebras is: "When can the uniform Kummer algebras underlying the cyclotomic algebras be represented as cyclotomic division algebras?" A look at our representation of the uniform Kummer algebras over \mathbb{Q} shows that this does not happen in general. Progress made by the author in determining when this does happen will be published at a later date.

References

1. Albert, A.A.: Structure of Algebras. Providence, R.I.: Amer. Math. Soc. 1961
2. Cassels, J.W.S., Fröhlich, A.: Algebraic Number Theory. Proceedings of an Instructional Conference (Brighton 1965). New York: Academic Press 1967
3. Chevalley, C.: La théorie du symbole de restes normiques. *J. Reine Angew. Math.* **169**, 140–157 (1933)
4. Chevalley, C.: Sur la théorie du corps de classes dans les corps finis et les corps locaux. *J. Fac. Sci. Univ. Tokyo* **2**, 365–476 (1933)
5. Goldstein, L.J.: Analytic Number Theory. Englewood Cliffs, N.J.: Prentice Hall 1971
6. Hasse, H.: Über p -adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlensysteme. *Math. Ann.* **104**, 495–534 (1931)
7. Janusz, G.: The Schur Group of an Algebraic Number Field. *Ann. of Math.* **103**, 253–281 (1976)
8. Janusz, G.: Algebraic Number Fields. New York: Academic Press 1973
9. Mollin, R.: Algebras with Uniformly Distributed Invariants. *J. Algebra* **44**, 271–282 (1977)

10. Mollin, R.: Uniform Distribution and the Schur Subgroup. *J. Algebra* **42**, 261–277 (1976)
11. Mollin, R.: Uniform Distribution and Real Fields. *J. Algebra* **43**, 155–167 (1976)
12. Mollin, R.: $U(K)$ for a Quadratic Field K . *Comm. Algebra* **4**, (8) 747–759 (1976)
13. Mollin, R.: Generalized Uniform Distribution of Hasse Invariants. *Comm. Algebra* **5** (3), 245–266 (1977)
14. Mollin, R.: Herstein's Conjecture, Automorphisms and the Schur Group. *Comm. Algebra* **6** (3), 237–248 (1978)
15. Mollin, R.: The Schur group of a Field of Characteristic Zero. *Pacific J. Math.* **76** (2), 471–478 (1978)
16. Mollin, R.: Induced Elements in the Schur Group. Preprint
17. Reiner, I.: *Maximal Orders*. New York: Academic Press 1975
18. Ribenboim, P.: *Algebraic Numbers*. New York: Wiley-Interscience 1972
19. Witt, E.: Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlkörper. *J. Reine Angew. Math.* **190**, 231–245 (1952)
20. Yamada, T.: The Schur Subgroup of the Brauer Group. *Lecture Notes in Mathematics* No. **397**. Berlin-Heidelberg-New York: Springer 1974

Received July 31, 1978

Note Added in Proof

January 9, 1979. The above problem has been solved as of this date.

