ISRAEL JOURNAL OF MATHEMATICS 96 (1996), 243–258

SUMS OF CORESTRICTIONS OF CYCLIC ALGEBRAS

BY

Burton Fein*

Department of Mathematics, Oregon State University
Corvallis, Oregon 97331, USA
e-mail: fein@math.orst.edu

AND

Murray Schacher**

Department of Mathematics, University of California at Los Angeles
Los Angeles, California 90024, USA
e-mail: mms@math.ucla.edu

In memory of S.A. Amitsur, our teacher, friend, collaborator, and inspiration.

ABSTRACT

By a cyclic layer of a finite Galois extension, E/K, of fields one means a cyclic extension, L/F, of fields where $E \supseteq L \supset F \supseteq K$. Let $\mathcal{C}(E/K)$ denote the subgroup of the relative Brauer group, $\mathrm{Br}(E/K)$, generated by the various subgroups $\mathrm{cor}(\mathrm{Br}(L/F))$ as L/F ranges over all cyclic layers of E/K and where cor denotes the corestriction map into $\mathrm{Br}(E/K)$. We show that for K global, $[\mathrm{Br}(E/K) : \mathcal{C}(E/K)] < \infty$ and we produce examples where $\mathcal{C}(E/K) \neq \mathrm{Br}(E/K)$.

Let E be a finite Galois extension of a field K with Galois group $\mathcal{G}$ and let $\mathrm{Br}(E/K)$, the relative Brauer group of E/K, denote the subgroup of the Brauer group, $\mathrm{Br}(K)$, of K consisting of those Brauer classes of finite dimensional central simple K-algebras which are split by E. If $\mathcal{G}$ is cyclic, the structure of $\mathrm{Br}(E/K)$ is well understood; one has $\mathrm{Br}(E/K) \cong K^*/\mathrm{N}(E^*)$ where N denotes the norm map from E to K [P, Proposition 15.1b]. For arbitrary E/K, however, very

* Supported in part by NSA Grant No. MDA904-95-H-1054.
** Supported in part by NSA Grant No. MDA904-95-H-1022.
Received March 15, 1995

little is known about the structure of $\mathrm{Br}(E/K)$. Perhaps the most successful technique for obtaining results in the general case involves the corestriction map from cyclic layers of E/K. In this paper we are concerned with the question of whether "most" elements of $\mathrm{Br}(E/K)$ are obtained in this manner.

By a cyclic layer of E/K we mean a Galois extension of fields L/F with cyclic Galois group where $E \supseteq L \supset F \supseteq K$. Let cor_K^F denote the corestriction homomorphism from $\mathrm{Br}(F)$ to $\mathrm{Br}(K)$; one verifies easily that $\mathrm{cor}_K^F(\mathrm{Br}(L/F)) \subseteq \mathrm{Br}(E/K)$. Let $\mathcal{C}(E/K)$ denote the subgroup of $\mathrm{Br}(E/K)$ generated by the various subgroups $\mathrm{cor}_K^F(\mathrm{Br}(L/F))$ taken over all cyclic layers L/F of E/K. Several results in the literature assert that, under mild hypotheses on K, $\mathrm{Br}(E/K)$ is necessarily infinite if $E \neq K$; these hypotheses include K finitely generated over a global field [FKS, Theorem 8] and K the function field of an absolutely irreducible variety over a field M where the transcendence degree of K over M is at least two [FS, Corollary 5]. These results are obtained by showing that $\mathcal{C}(E/K)$ is infinite. This raises the basic question with which we are concerned here: what is the relationship between $\mathrm{Br}(E/K)$ and $\mathcal{C}(E/K)$? In this generality this question appears unapproachable with our present knowledge of relative Brauer groups. We focus here on the case when K is a global field where more detailed information about relative Brauer groups is available. For K global, we show that $\mathcal{C}(E/K)$ contains all elements of $\mathrm{Br}(E/K)$ of prime order and that $\mathcal{C}(E/K)$ always has finite index in $\mathrm{Br}(E/K)$. We also show that if E is everywhere unramified over K and every Sylow subgroup of $\mathcal{G}$ either has prime exponent or is abelian, then $\mathrm{Br}(E/K) = \mathcal{C}(E/K)$; in contrast, if E is everywhere unramified over K and $\mathcal{G}$ is the quaternion group of order 8, then $\mathrm{Br}(E/K) \neq \mathcal{C}(E/K)$.

Throughout this paper K will be a global field and E will be a fixed finite Galois extension of K with Galois group $\mathcal{G}$. By a global field we mean either an algebraic number field or an algebraic function field of transcendence degree one over a finite field. Before establishing the notation we will be using, we briefly discuss the role that ramification plays in the questions we are concerned with.

It is not difficult to show (see Proposition 3 below) that $\mathcal{C}(E/K)$ has exponent equal to the exponent of $\mathcal{G}$. (By the exponent of a group we mean the least common multiple of the orders of its elements.) It is possible, however, for $\mathrm{Br}(E/K)$ to have larger exponent. As an illustration of this, $\mathcal{C}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ has exponent 2 but $\mathrm{Br}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ contains elements of order 4 [S, Theorem 3.1]. Elements of $\mathrm{Br}(E/K)$ having order not dividing the exponent of $\mathcal{G}$ necessarily have a non-zero Hasse invariant at a prime of K ramified in E. In particular, elements of $\mathrm{Br}(E/K)$ "unramified" in the sense that they have non-zero Hasse invariant only at primes of K unramified in E have order dividing the exponent of $\mathcal{G}$ and so are candidates to be in $\mathcal{C}(E/K)$. For this reason, we focus attention on these "unramified" elements. If E is everywhere unramified over K, then all elements of $\mathrm{Br}(E/K)$ are "unramified" in the above sense.

Let π be a prime of K and let $E \supseteq L \supseteq K$. We denote the completion of K at π by K_π. If γ is a prime of L extending π, we refer to $[L_\gamma\colon K_\pi]$ as the local degree of γ over K. We say that π is unramified in L if all extensions of π to L are unramified over K. We define π to be **undecomposed** in L if π has a unique extension δ to L which is unramified over K; if π is undecomposed in L and δ extends π to L, then δ has local degree $[L\colon K]$ over K. Suppose π is unramified in E and δ is some extension of π to E. Then $\mathrm{Gal}(E_\delta/K_\pi)$ is cyclic with canonical generator the Frobenius automorphism, say σ, of δ. A different choice of δ yields a conjugate of σ as corresponding Frobenius automorphism and all conjugates of σ arise in this way.

We will use freely the basic results of Albert, Brauer, Hasse, and Noether which classify the elements of $\mathrm{Br}(K)$ by means of Hasse invariants; we refer the reader to [P, Chapter 18] for an exposition of this theory. We summarize below several of the main results of this theory that we will frequently use.

Let $\alpha \in \mathrm{Br}(K)$. If π is a prime of K, we denote the Hasse invariant of α at π by $\mathrm{inv}_\pi(\alpha)$. Then $\mathrm{inv}_\pi(\alpha) \in \mathbb{Q}/\mathbb{Z}$ and we view $\mathrm{inv}_\pi(\alpha)$ as a rational number in lowest terms in $[0,1)$. Let $\mathcal{H}$ denote the subgroup of $\bigoplus(\mathbb{Q}/\mathbb{Z})_\pi$, the direct sum of copies of $\mathbb{Q}/\mathbb{Z}$ indexed by the set of primes π of K, consisting of those elements (b_π) such that $\sum_\pi b_\pi = 0$ and such that $b_\pi \in \{0, 1/2\}$ if π is real Archimedean and $b_\pi = 0$ if π is complex. The map $\mathrm{INV}\colon\ \mathrm{Br}(K) \longrightarrow \mathcal{H}$ defined by $\mathrm{INV}(\alpha) = (\mathrm{inv}_\pi(\alpha))$ is an isomorphism between $\mathrm{Br}(K)$ and $\mathcal{H}$ [P, Theorem 18.5]. The denominator of $\mathrm{inv}_\pi(\alpha)$ is called the **local index** of α at π and denoted $\mathrm{l.i.}_\pi(\alpha)$. The order of α in $\mathrm{Br}(K)$ is denoted by $\exp(\alpha)$; $\exp(\alpha)$ is the least common multiple, taken over all primes of K, of the local indices of α [P, Proposition 18.6 and Theorem 18.6]. Let L be a finite separable extension of K. Then L splits α if and only if for all primes π of K, $\mathrm{l.i.}_\pi(\alpha)$ divides $[L_\delta\colon K_\pi]$ for all extensions δ of π to L [P, Corollary 18.4b]. If L splits α, then $\exp(\alpha)$ divides $[L\colon K]$ [P, Proposition 14.4a]. p will always denote a prime. We denote the p-primary component of $\mathrm{Br}(L/K)$ by $\mathrm{Br}(L/K)_p$. $\mathrm{Br}(L/K)$ is the direct sum of its subgroups $\mathrm{Br}(L/K)_p$ as p ranges over the finitely many primes dividing $[L\colon K]$.

Let $\beta \in \mathrm{Br}(L)$. In what follows, we will make frequent use of the following important formula for the Hasse invariants of $\mathrm{cor}_K^L(\beta) \in \mathrm{Br}(K)$; for a proof of this result, see [CF, page 187].

LEMMA 0: *Let L be a finite separable extension of K, let $\beta \in \mathrm{Br}(L)$, let π be a prime of K, and let $\pi_1, \dots, \pi_t$ be the primes of L extending π. Then*

$$\mathrm{inv}_\pi(\mathrm{cor}_K^L(\beta)) = \sum_{i=1}^{t} \mathrm{inv}_{\pi_i}(\beta)$$

It will be convenient to have a notation for the "unramified" elements of $\mathrm{Br}(E/K)$.

Definition: $\mathrm{Br}(E/K)_{\mathrm{un}}$ is the subgroup of $\mathrm{Br}(E/K)$ consisting of those $\alpha \in \mathrm{Br}(E/K)$ such that if $\mathrm{inv}_\pi(\alpha) \neq 0$, then π is unramified in E.

We begin our discussion by singling out particularly convenient sets of generators for $\mathrm{Br}(E/K)$ and $\mathrm{Br}(E/K)_{\mathrm{un}}$.

Definition: An element $\alpha \in \mathrm{Br}(K)$ is **basic** if it has non-zero Hasse invariant at precisely two primes of K.

We note that if $\alpha \in \mathrm{Br}(K)$ is basic and π_1 and π_2 are the primes of K at which α has non-zero Hasse invariant, then $\mathrm{inv}_{\pi_1}(\alpha) = -\mathrm{inv}_{\pi_2}(\alpha)$. Also, if π_1 and π_2 are distinct primes of K and n is a possible value for the local index at π_1 and π_2 of an element of $\mathrm{Br}(K)$, then there exists a basic element of order n having non-zero Hasse invariants precisely at π_1 and π_2. Both assertions are immediate consequences of the Hasse-Brauer-Noether-Albert Theorem [P, Theorem 18.5].

LEMMA 1: *Let $\beta \in \mathrm{Br}(E/K)$ (respectively, $\mathrm{Br}(E/K)_{\mathrm{un}}$) have order m. Then β can be expressed as a sum $\sum_j \alpha_j$ of basic elements of $\mathrm{Br}(E/K)$ (respectively, $\mathrm{Br}(E/K)_{\mathrm{un}}$) of prime power order dividing m.*

Proof: We give the proof for $\mathrm{Br}(E/K)$; the argument for $\mathrm{Br}(E/K)_{\mathrm{un}}$ is identical. We may clearly assume that $\exp(\beta) = p^r$ where p is prime. We proceed by induction on the number n of primes π of K with $\mathrm{inv}_\pi(\beta) \neq 0$. Then $n \geq 2$ and if $n = 2$, then β is already a basic element of the same order. Assume inductively that the result is true for elements of $\mathrm{Br}(E/K)$ with non-zero Hasse invariants at less than n primes of K and suppose $n > 2$. There exists a prime π_1 of K with $\mathrm{l.i.}_{\pi_1}(\beta) = p^r$. Since the sum of the Hasse invariants of β equals 0, there must be at least two such primes, say π_1 and π_2. Let $\alpha \in \mathrm{Br}(K)$ be the basic element such that $\mathrm{inv}_{\pi_1}(\alpha) = -\mathrm{inv}_{\pi_1}(\beta)$ and $\mathrm{inv}_{\pi_2}(\alpha) = \mathrm{inv}_{\pi_1}(\beta)$. Since $\beta \in \mathrm{Br}(E/K)$, all extensions of π_i in E have local degree divisible by p^r for $i = 1, 2$. It follows that E also splits α and so α is a basic element of $\mathrm{Br}(E/K)$ of order p^r. Let $\gamma = \beta + \alpha \in \mathrm{Br}(E/K)$. Then $\mathrm{inv}_{\pi_1}(\gamma) = \mathrm{inv}_{\pi_1}(\beta) + \mathrm{inv}_{\pi_1}(\alpha) = 0$ and so γ has non-zero Hasse invariants at less than n primes of K. By our inductive hypothesis, γ is a sum of basic elements of $\mathrm{Br}(E/K)$, each of order dividing p^r. But then $\beta = (p^r - 1)\alpha + \gamma$ is a sum of basic elements of $\mathrm{Br}(E/K)$ of order dividing p^r, completing the induction. ∎

As an application of Lemma 1, we show that $\mathrm{Br}(E/K)_{\mathrm{un}}$ has finite index in $\mathrm{Br}(E/K)$.

Proposition 2: $[\mathrm{Br}(E/K)\colon \mathrm{Br}(E/K)_{\mathrm{un}}] < \infty$.

Proof: It is clearly enough to prove that for each prime p, $(\mathrm{Br}(E/K)_{\mathrm{un}})_p$ has finite index in $\mathrm{Br}(E/K)_p$. Let p be prime and let $\mathcal{P} = \{\pi_1, \dots, \pi_t\}$ denote the set of primes of K ramified in E. Let $\mathcal{R}_1$ denote the set of basic elements of $\mathrm{Br}(E/K)_p$ having non-zero Hasse invariant only at primes in $\mathcal{P}$. $\mathcal{R}_1$ is finite since $\mathcal{P}$ is finite and the order of any element of $\mathcal{R}_1$ divides $[E\colon K]$. For each u with p^u dividing $[E\colon K]$ and each i with $1 \le i \le t$, choose, if such exists, a basic element of $\mathrm{Br}(E/K)_p$ not in $\mathcal{R}_1$ which has order p^u and non-zero Hasse invariant at π_i. Let $\mathcal{R}_2$ be the (finite) set of basic elements chosen. By Lemma 1, it suffices to prove that for each basic element β of $\mathrm{Br}(E/K)_p$, $\beta + (\mathrm{Br}(E/K)_{\mathrm{un}})_p$ is in the subgroup of $\mathrm{Br}(E/K)_p/(\mathrm{Br}(E/K)_{\mathrm{un}})_p$ generated by the finitely many cosets $\alpha + (\mathrm{Br}(E/K)_{\mathrm{un}})_p$ for $\alpha \in \mathcal{R}_1 \cup \mathcal{R}_2$.

Suppose β is a basic element of $\mathrm{Br}(E/K)_p$ and suppose that π and δ are the primes of K at which β has non-zero Hasse invariant. If π and δ are both in $\mathcal{P}$, then $\beta \in \mathcal{R}_1$; if π and δ are both unramified in E, then $\beta \in (\mathrm{Br}(E/K)_{\mathrm{un}})_p$. Assume then that $\pi \in \mathcal{P}$ and δ is unramified in E. Let $\mathrm{inv}_\pi(\beta) = a/p^v$. Since $\beta \notin \mathcal{R}_1$, by our choice of $\mathcal{R}_2$ there exists a basic element $\alpha \in \mathcal{R}_2$ with $\mathrm{inv}_\pi(\alpha) = b/p^v$ for some b. Let γ be the other prime of K at which α has non-zero Hasse invariant. Since $\alpha \in \mathcal{R}_2$, γ is unramified in E. Since $(a,p) = (b,p) = 1$, there exists c with $bc \equiv a \pmod{p^v}$. But then $\mathrm{inv}_\pi(\beta - c\alpha) = 0$. It follows that $\beta - c\alpha$ can have non-zero Hasse invariant only at δ and γ and so $\beta - c\alpha \in (\mathrm{Br}(E/K)_{\mathrm{un}})_p$. Thus $\beta + (\mathrm{Br}(E/K)_{\mathrm{un}})_p = c\alpha + (\mathrm{Br}(E/K)_{\mathrm{un}})_p$. ∎

For the convenience of the reader, we isolate two definitions made earlier.

Definition:

(1) A **cyclic layer** L/F of E/K is a Galois extension of fields L/F with cyclic Galois group with $E \supseteq L \supset F \supseteq K$.

(2) $\mathcal{C}(E/K)$ is defined to be the subgroup of $\mathrm{Br}(K)$ generated by the various subgroups $\mathrm{cor}_K^F(\mathrm{Br}(L/F))$ taken over all cyclic layers of E/K.

We next justify several assertions made in the introduction.

PROPOSITION 3:

(1) *Let L/F be a cyclic layer of E/K. Then $\mathrm{cor}_K^F(\mathrm{Br}(L/F)) \subseteq \mathrm{Br}(E/K)$.*

(2) *The exponent of $\mathcal{C}(E/K)$ equals the exponent of $\mathcal{G}$.*

(3) *The exponent of $\mathrm{Br}(E/K)_{\mathrm{un}}$ equals the exponent of $\mathcal{G}$.*

Proof: (1) Let $\beta \in \mathrm{Br}(L/F)$. Then β is split by L so β is split by E. Thus $\beta \in \mathrm{Br}(E/F) \cong H^2(\mathcal{H}, E^*)$ where $\mathcal{H} = \mathrm{Gal}(E/F)$. $\mathrm{cor}_K^F\colon \mathrm{Br}(E/F) \longrightarrow \mathrm{Br}(K)$ corresponds to the cohomological corestriction map $\mathrm{cor}_{\mathcal{H}}^{\mathcal{G}}\colon H^2(\mathcal{H}, E^*) \longrightarrow H^2(\mathcal{G}, E^*) \cong \mathrm{Br}(E/K)$. It follows that $\mathrm{cor}_K^F(\mathrm{Br}(L/F)) \subseteq \mathrm{Br}(E/K)$.

(2) Suppose first that L/F is a cyclic layer of E/K and $\beta \in \mathrm{Br}(L/F)$. Let σ generate $\mathrm{Gal}(L/F)$ and let τ be some extension of σ to E. Then $\tau \in \mathrm{Gal}(E/F) \subseteq \mathcal{G}$. If τ has order m, then σ^m is the identity automorphism of L and so the order of σ, $[L\colon F]$, divides m. In particular, $[L\colon F]$ divides the exponent of $\mathcal{G}$. Since cor_K^F is a homomorphism, $\exp(\mathrm{cor}_K^F(\beta))$ divides $\exp(\beta)$. Since $\exp(\beta)$ divides $[L\colon F]$, $\exp(\mathrm{cor}_K^F(\beta))$ divides the exponent of $\mathcal{G}$ and so the exponent of $\mathcal{C}(E/K)$ divides the exponent of $\mathcal{G}$. Conversely, suppose p is a prime and p^r divides the exponent of $\mathcal{G}$. We must produce an element of $\mathcal{C}(E/K)$ of order p^r. By assumption, there exists $\sigma \in \mathcal{G}$ of order p^r. By the Tchebotarev Density Theorem [J, Theorem 10.4], there exist infinitely many primes of E having σ as Frobenius automorphism. Let π_1 and π_2 be distinct primes of K unramified in E and having extensions δ_1 and δ_2 to E with σ as Frobenius automorphism. Let $F = E^\sigma$ and let γ_1 and γ_2 be, respectively, the restrictions of δ_1 and δ_2 to F. Then γ_i has local degree 1 over K and is undecomposed in E. Thus $[E_{\delta_i}\colon F_{\gamma_i}] = p^r$ for $i = 1, 2$. Let $\beta \in \mathrm{Br}(F)$ be a basic element having local index p^r at γ_1 and γ_2. Then E splits β so $\beta \in \mathrm{Br}(E/F)$. Since E/F is a cyclic layer of E/K, $\mathrm{cor}_K^F(\beta)$ is an element of $\mathcal{C}(E/K)$; $\mathcal{C}(E/K)$ has order p^r by Lemma 0.

(3) Since only finitely many primes of K ramify in E, the element β constructed in the proof of (2) can be chosen so that $\mathrm{cor}_K^F(\beta) \in \mathrm{Br}(E/K)_{\mathrm{un}}$. It follows that the exponent of $\mathcal{G}$ divides the exponent of $\mathrm{Br}(E/K)_{\mathrm{un}}$. Conversely, suppose p is

a prime and $\alpha \in \mathrm{Br}(E/K)_{\mathrm{un}}$ has order p^t. We must show that $\mathcal{G}$ contains an element of order p^t. Let π be a prime of K at which α has local index p^t and let δ be an extension of π to E. Since $\alpha \in \mathrm{Br}(E/K)_{\mathrm{un}}$, π is unramified in E. Let σ be the Frobenius automorphism of δ, let $F = E^{\sigma}$, and let γ denote the restriction of δ to F. Then γ has local degree 1 over K and is undecomposed in E. Since E splits α, p^t divides $[E_\delta\colon F_\gamma]$. Since $\mathrm{Gal}(E_\delta/F_\gamma) \subseteq \mathcal{G}$ is cyclic, it contains an element of order p^t. Thus $\mathcal{G}$ contains an element of order p^t. ∎

Our next result gives a sufficient condition for basic elements of $\mathrm{Br}(E/K)_{\mathrm{un}}$ to be elements of $\mathcal{C}(E/K)$.

PROPOSITION 4: *Let α be a basic element of $\mathrm{Br}(E/K)_{\mathrm{un}}$ and let π_1 and π_2 be the two primes of K where α has non-zero Hasse invariant. Let σ_i be the Frobenius automorphism of some extension of π_i to E for $i = 1, 2$. If σ_1 and σ_2 are conjugate in $\mathcal{G}$, then $\alpha \in \mathcal{C}(E/K)$.*

Proof: Assume that σ_1 and σ_2 are conjugate in $\mathcal{G}$. Since every conjugate of σ_2 is the Frobenius automorphism of some extension of π_2 to E, we may assume that $\sigma_1 = \sigma_2$. Let $\sigma = \sigma_1 = \sigma_2$ and let δ_i be an extension of π_i to E having σ as Frobenius automorphism for $i = 1, 2$. Let $F = E^{\langle\sigma\rangle}$ and let γ_i denote the restriction of δ_i to F for $i = 1, 2$. Then $F_{\gamma_i} = K_{\pi_i}$ and γ_i is undecomposed in E for $i = 1, 2$. Let $\beta \in \mathrm{Br}(F)$ be the basic element such that $\mathrm{inv}_{\gamma_i}(\beta) = \mathrm{inv}_{\pi_i}(\alpha)$ for $i = 1, 2$. Since E splits α, the local degree over K of every extension to E of π_1 and π_2 is divisible by $\exp(\alpha)$. It follows that every extension to E of γ_1 and γ_2 has local degree over F divisible by $\exp(\beta) = \exp(\alpha)$. Thus E splits β and so $\beta \in \mathrm{Br}(E/F)$. By definition of β and Lemma 0, $\alpha = \mathrm{cor}_K^F(\beta)$. Since E/F is a cyclic layer of E/K, $\alpha \in \mathcal{C}(E/K)$. ∎

We are now able to prove our first main result.

THEOREM 5: *Let E be a finite Galois extension of the global field K. Then $\mathcal{C}(E/K)$ is a subgroup of $\mathrm{Br}(E/K)$ of finite index.*

Proof: Suppose for every prime p that $(\mathrm{Br}(E/K)_{\mathrm{un}}/(\mathcal{C}(E/K) \cap \mathrm{Br}(E/K)_{\mathrm{un}}))_p$ is finitely generated. Since the order of any element of $\mathrm{Br}(E/K)$ divides $[E\colon K]$, it follows that $\mathcal{C}(E/K) \cap \mathrm{Br}(E/K)_{\mathrm{un}}$ has finite index in $\mathrm{Br}(E/K)_{\mathrm{un}}$. By Lemma

2, $\mathrm{Br}(E/K)/\mathrm{Br}(E/K)_{\mathrm{un}}$ is a finite group. It follows that

$$\begin{aligned}&|\mathrm{Br}(E/K)/\mathcal{C}(E/K)|\\ &=|\mathrm{Br}(E/K)/\mathcal{C}(E/K)\,\mathrm{Br}(E/K)_{\mathrm{un}}|\cdot|\mathcal{C}(E/K)\,\mathrm{Br}(E/K)_{\mathrm{un}}/\mathcal{C}(E/K)|\\ &\leq|\mathrm{Br}(E/K)/\mathrm{Br}(E/K)_{\mathrm{un}}|\cdot|\mathrm{Br}(E/K)_{\mathrm{un}}/(\mathcal{C}(E/K)\cap\mathrm{Br}(E/K)_{\mathrm{un}})|<\infty.\end{aligned}$$

It remains to show that there exists a finite set of generators for the p-primary component of $\mathrm{Br}(E/K)_{\mathrm{un}}/(\mathcal{C}(E/K)\cap\mathrm{Br}(E/K)_{\mathrm{un}})$. Let $\mathcal{P}$ be a Sylow p-subgroup of $\mathcal{G}=\mathrm{Gal}(E/K)$. For each $(\sigma_1,\sigma_2)\in\mathcal{P}\times\mathcal{P}$, choose a fixed ordered pair (π_1,π_2) of primes of K unramified in E with $\pi_1\neq\pi_2$ such that, for $i=1,2$, σ_i is the Frobenius automorphism of some extension to E of π_i; the existence of π_1 and π_2 is a consequence of the Tchebotarev Density Theorem [J, Theorem 10.4]. We denote (π_1,π_2) by $\pi(\sigma_1,\sigma_2)$. For each $(\sigma_1,\sigma_2)\in\mathcal{P}\times\mathcal{P}$, let $p^r=\min\{|\langle\sigma_1\rangle|,|\langle\sigma_2\rangle|\}$ and let $\alpha(\sigma_1,\sigma_2)$ be the basic element of $\mathrm{Br}(K)$ such that $\mathrm{inv}_{\pi_i}(\alpha(\sigma_1,\sigma_2))=(-1)^i/p^r$ for $i=1,2$. Since σ_i is the Frobenius automorphism of some extension δ_i to E of π_i, δ_i has local degree $|\langle\sigma_i\rangle|$ over K. Since E is Galois over K, every extension of π_i to E has local degree divisible by p^r. It follows that $\alpha(\sigma_1,\sigma_2)$ is a basic element of $\mathrm{Br}(E/K)_{\mathrm{un}}$ of order p^r. We will show that the cosets $\alpha(\sigma_1,\sigma_2)+(\mathcal{C}(E/K)\cap\mathrm{Br}(E/K)_{\mathrm{un}})$ for $(\sigma_1,\sigma_2)\in\mathcal{P}\times\mathcal{P}$ generate the p-primary component of $\mathrm{Br}(E/K)_{\mathrm{un}}/(\mathcal{C}(E/K)\cap\mathrm{Br}(E/K)_{\mathrm{un}})$. By Lemma 1, it suffices to show that if β is a basic element of p-power order in $\mathrm{Br}(E/K)_{\mathrm{un}}$, then $\beta-c\alpha(\sigma_1,\sigma_2)\in\mathcal{C}(E/K)\cap\mathrm{Br}(E/K)_{\mathrm{un}}$ for some integer c and some $(\sigma_1,\sigma_2)\in\mathcal{P}\times\mathcal{P}$.

Let $\beta\in\mathrm{Br}(E/K)_{\mathrm{un}}$ be a basic element of order p^t and let θ_1 and θ_2 be the primes of K at which β has non-zero Hasse invariant. Let $\mathrm{inv}_{\theta_1}(\beta)=b/p^t$ where $(b,p)=1$. Then $\mathrm{inv}_{\theta_2}(\beta)=-b/p^t$. Since the Sylow subgroups of $\mathcal{G}$ are conjugate, each θ_i has an extension to E whose Frobenius automorphism σ_i is in $\mathcal{P}$. Let $(\pi_1,\pi_2)=\pi(\sigma_1,\sigma_2)$ and let $\alpha=\alpha(\sigma_1,\sigma_2)$. Then $\exp(\alpha)=p^r$ where $p^r=\min\{|\langle\sigma_1\rangle|,|\langle\sigma_2\rangle|\}$. Moreover, the local degree over K of each extension to E of θ_i divides p^r. Since E splits β, $r\geq t$. We will show that $\beta+bp^{r-t}\alpha(\sigma_1,\sigma_2)\in\mathcal{C}(E/K)\cap\mathrm{Br}(E/K)_{\mathrm{un}}$.

By definition, $\mathrm{inv}_{\pi_1}(\alpha)=-1/p^r$ and $\mathrm{inv}_{\pi_2}(\alpha)=1/p^r$. We define $\alpha_i\in\mathrm{Br}(K)$ for $i=1,2$ as follows. If $\theta_i=\pi_i$, we set $\alpha_i=0$. If $\theta_i\neq\pi_i$, we define α_i to be the basic element of $\mathrm{Br}(K)$ such that $\mathrm{inv}_{\theta_i}(\alpha_i)=(-1)^{i+1}b/p^t$ and $\mathrm{inv}_{\pi_i}(\alpha_i)=(-1)^ib/p^t$. Then $\beta+bp^{r-t}\alpha$ and $\alpha_1+\alpha_2$ have the same Hasse invariants and so $\beta+bp^{r-t}\alpha(\sigma_1,\sigma_2)=\alpha_1+\alpha_2$. Since E splits both β and α, every prime of E extending one of θ_1, θ_2, π_1, or π_2 has local degree over K divisible by p^t. Thus each $\alpha_i \in \mathrm{Br}(E/K)_{\mathrm{un}}$. By Proposition 4, each $\alpha_i \in \mathcal{C}(E/K)$ and so $\beta + bp^{r-t}\alpha(\sigma_1, \sigma_2) = \alpha_1 + \alpha_2 \in \mathcal{C}(E/K) \cap \mathrm{Br}(E/K)_{\mathrm{un}}$. ∎

We next turn to the question of which elements of $\mathrm{Br}(E/K)$ are in $\mathcal{C}(E/K)$ and begin with an easy reduction result.

Lemma 6: *Suppose $E \supseteq M \supseteq K$ and α is a basic element of $\mathrm{Br}(E/K)$. Assume that there exists $\beta \in \mathcal{C}(E/M)$ with $\mathrm{cor}_K^M(\beta) = \alpha$. Then $\alpha \in \mathcal{C}(E/K)$.*

Proof: By assumption, there exist cyclic layers $L_1/F_1, \dots, L_t/F_t$ of E/M and elements β_j of $\mathrm{Br}(L_j/F_j)$ for $j = 1, \dots, t$ such that $\beta = \sum_{j=1}^t \mathrm{cor}_M^{F_j}(\beta_j)$. But then

$$\alpha = \mathrm{cor}_K^M(\beta) = \sum_{j=1}^t \mathrm{cor}_K^M \mathrm{cor}_M^{F_j}(\beta_j) = \sum_{j=1}^t \mathrm{cor}_K^{F_j}(\beta_j) \in \mathcal{C}(E/K)$$

since L_j/F_j is also a cyclic layer of E/K. ∎

We next reduce to the case when $\mathcal{G}$ is a p-group.

Proposition 7: *Let $\mathcal{P}$ be a Sylow p-subgroup of $\mathcal{G}$ and let $M = E^{\mathcal{P}}$.*

(1) *If $\mathrm{Br}(E/M) = \mathcal{C}(E/M)$, then $\mathrm{Br}(E/K)_p = \mathcal{C}(E/K)_p$.*
(2) *If $\mathrm{Br}(E/M)_{\mathrm{un}} \subseteq \mathcal{C}(E/M)$, then $(\mathrm{Br}(E/K)_{\mathrm{un}})_p \subseteq \mathcal{C}(E/K)_p$.*
(3) *If every element of order p in $\mathrm{Br}(E/M)$ is in $\mathcal{C}(E/M)$, then every element of order p in $\mathrm{Br}(E/K)$ is in $\mathcal{C}(E/K)$.*

Proof: We only prove (1); (2) and (3) are proved by a similar argument. Assume that $\mathrm{Br}(E/M) = \mathcal{C}(E/M)$. By Lemma 1, it is sufficient to prove that all basic elements of $\mathrm{Br}(E/K)_p$ lie in $\mathcal{C}(E/K)$. Let α be a basic element in $\mathrm{Br}(E/K)_p$ and let π_1 and π_2 be the primes of K at which α has non-zero Hasse invariant. Fix i with $1 \leq i \leq 2$. The sum of the local degrees over K of the various extensions of π_i to M equals $[E\colon M]$ [W, Theorem 2-4-6]. Since $[E\colon M] = |\mathcal{P}|$, $(p, [M\colon K]) = 1$. It follows that there exists a prime γ_i of M having local degree over K which is prime to p. Let δ_i denote an extension of γ_i to E. Since E splits α, $\exp(\alpha)$ divides $[E_{\delta_i}\colon K_{\pi_i}] = [E_{\delta_i}\colon M_{\gamma_i}][M_{\gamma_i}\colon K_{\pi_i}]$ and so $\exp(\alpha)$ divides $[E_{\delta_i}\colon M_{\gamma_i}]$ for $i = 1, 2$. Let $\beta \in \mathrm{Br}(M)$ be the basic element such that $\mathrm{inv}_{\gamma_i}(\beta) = \mathrm{inv}_{\pi_i}(\alpha)$ for $i = 1, 2$. Then E splits β so $\beta \in \mathcal{C}(E/M)$ by hypothesis. Since $\mathrm{cor}_K^M(\beta) = \alpha$ by Lemma 0, $\alpha \in \mathcal{C}(E/K)$ by Lemma 6. ∎

We will see later that there exist examples where, with context as in Proposition 7, $\mathrm{Br}(E/K)_p = \mathcal{C}(E/K)_p$ but $\mathrm{Br}(E/M)_p \neq \mathcal{C}(E/M)_p$. We next consider a special case when $\mathcal{G}$ is a 2-generator abelian p-group.

LEMMA 8: *Assume that $\mathcal{G} = \langle\sigma_1\rangle \times \langle\sigma_2\rangle$ where $|\langle\sigma_i\rangle| = p^r$ for $i = 1, 2$. Let α be a basic element of $\mathrm{Br}(E/K)$ of order p^r and let π_1 and π_2 be the primes of K at which α has non-zero Hasse invariant. Let δ_1 and δ_2 be primes of E extending π_1 and π_2, respectively. Assume that one of the following holds:*

(1) $\mathrm{Gal}(E_{\delta_i}/K_{\pi_i}) = \langle\sigma_i\rangle$ *for* $i = 1, 2$;

(2) $\mathrm{Gal}(E_{\delta_i}/K_{\pi_i}) = \langle\sigma_1\rangle \times \langle\sigma_2\rangle$ *for* $i = 1, 2$;

(3) $\mathrm{Gal}(E_{\delta_1}/K_{\pi_1}) = \langle\sigma_1\rangle \times \langle\sigma_2\rangle$ *and* $\mathrm{Gal}(E_{\delta_2}/K_{\pi_2}) = \langle\sigma_2\rangle$;

(4) $\mathrm{Gal}(E_{\delta_2}/K_{\pi_2}) = \langle\sigma_1\rangle \times \langle\sigma_2\rangle$ *and* $\mathrm{Gal}(E_{\delta_1}/K_{\pi_1}) = \langle\sigma_1\rangle$.

Then $\alpha \in \mathcal{C}(E/K)$.

Proof: If (2) holds, then π_i is undecomposed in E^{σ_1} for $i = 1, 2$. Since $[E^{\sigma_1}\colon K] = p^r$, it follows that E^{σ_1} splits α. Since E^{σ_1}/K is a cyclic layer of E/K and $\alpha \in \mathrm{Br}(E^{\sigma_1}/K)$, $\alpha \in \mathcal{C}(E/K)$. Thus we may assume that either (1), (3), or (4) holds. Let $T = E^{\sigma_1\sigma_2}$. T/K is a cyclic layer of E/K and so it suffices to prove that T splits α. This is equivalent to showing that π_i is undecomposed in T for $i = 1, 2$. Let Z_i denote the decomposition field of π_i in T for $i = 1, 2$. We must show that $Z_1 = Z_2 = K$.

Suppose (1) or (3) holds. Since $\mathrm{Gal}(E_{\delta_2}/K_{\pi_2}) = \langle\sigma_2\rangle$, π_2 splits completely in E^{σ_2} but not in any proper extension of E^{σ_2} inside of E. Since π_2 also splits completely in Z_2, π_2 splits completely in $Z_2E^{\sigma_2}$. It follows that $Z_2 \subseteq E^{\sigma_2}$. But $Z_2 \subseteq T$ and so $Z_2 \subseteq T \cap E^{\sigma_2}$. Since $\mathcal{G} = \langle\sigma_1\sigma_2, \sigma_2\rangle$, $T \cap E^{\sigma_2} = K$ and so $Z_2 = K$ as was to be shown. If (1) holds, a similar argument shows that $Z_1 = K$ also. If (3) holds, then π_1 is undecomposed in E and so π_1 is undecomposed in T. In particular, $Z_1 = K$. The case when (4) holds follows by symmetry. ∎

We are finally in a position to prove that elements of $\mathrm{Br}(E/K)$ of prime order lie in $\mathcal{C}(E/K)$.

THEOREM 9: *Let E be a finite Galois extension of the global field K. Then $\mathcal{C}(E/K)$ contains all elements of $\mathrm{Br}(E/K)$ of prime order.*

Proof: By Proposition 7(3), we may assume that $\mathcal{G} = \mathrm{Gal}(E/K)$ is a p-group for some prime p. If $\mathcal{G}$ is cyclic, then E/K is a cyclic layer of E/K so $\alpha \in \mathcal{C}(E/K)$. Thus we may assume that $\mathcal{G}$ is not cyclic. By Lemma 1, it suffices to prove that basic elements of order p in $\mathrm{Br}(E/K)$ are in $\mathcal{C}(E/K)$. Let α be a basic element of order p in $\mathrm{Br}(E/K)$ and let π_1 and π_2 be the primes of K at which α has non-zero Hasse invariant. Let δ_i be an extension to E of π_i for $i = 1, 2$. Since E splits α, p divides $|\,\mathrm{Gal}(E_{\delta_i}/K_{\pi_i})|$ for $i = 1, 2$. Let σ_i be an element of $\mathrm{Gal}(E_{\delta_i}/K_{\pi_i})$ of order p for $i = 1, 2$. We show next that we may assume that $\mathcal{G} = \langle\sigma_1, \sigma_2\rangle$.

Let $\mathcal{H} = \langle\sigma_1, \sigma_2\rangle$, let $N = E^{\mathcal{H}}$, and let γ_i denote the restriction of δ_i to N for $i = 1, 2$. Let $\beta \in \mathrm{Br}(N)$ be the basic element of order p such that $\mathrm{inv}_{\gamma_i}(\beta) = \mathrm{inv}_{\pi_i}(\alpha)$. Then $\mathrm{cor}_K^N(\beta) = \alpha$. We claim that $\beta \in \mathrm{Br}(E/N)$. Let $N_i = E^{\sigma_i}$ and let λ_i denote the restriction of δ_i to N_i for $i = 1, 2$. Then $[E_{\delta_i}\colon (N_i)_{\lambda_i}] = p$ and so p divides $[E_{\delta_i}\colon N_{\gamma_i}]$ for $i = 1, 2$. Since E is a Galois extension of N, p divides the local degree over N of every extension of γ_i to E. It follows that E splits β. By Lemma 6, if $\beta \in \mathcal{C}(E/N)$, then $\alpha \in \mathcal{C}(E/K)$. Thus, replacing α by β, we may assume that $\mathcal{G} = \langle\sigma_1, \sigma_2\rangle$.

Let $\Phi(\mathcal{G})$ denote the Frattini subgroup of $\mathcal{G}$ and let M be the fixed field of $\Phi(\mathcal{G})$. Since $\mathcal{G}$ is a non-cyclic two generator p-group, M is a Galois extension of K with Galois group elementary abelian of order p^2. Let $\tau_i = \sigma_i\Phi(\mathcal{G}) \in \mathrm{Gal}(M/K)$ so $\mathrm{Gal}(M/K) = \langle\tau_1\rangle \times \langle\tau_2\rangle$. Since $\mathrm{Gal}(M/K)$ is not cyclic, $\sigma_i \notin \Phi(\mathcal{G})$ for $i = 1, 2$. In particular, for $i = 1, 2$, π_i does not split completely in M and so every extension of π_i to M has local degree over K divisible by p. It follows that $\alpha \in \mathrm{Br}(M/K)$. Since cyclic layers of M/K are also cyclic layers of E/K, we may assume that $E = M$.

We are now reduced to the following situation: $\mathrm{Gal}(E/K) = \langle\sigma_1\rangle \times \langle\sigma_2\rangle$ where σ_1 and σ_2 each have order p and $\sigma_i \in \mathrm{Gal}(E_{\delta_i}/K_{\pi_i})$ for $i = 1, 2$. Since σ_i has order p for $i = 1, 2$, one of the cases (1)–(4) of Lemma 8 must hold and so $\alpha \in \mathcal{C}(E/K)$. ∎

We turn next to the question of which elements of $\mathrm{Br}(E/K)_{\mathrm{un}}$ are in $\mathcal{C}(E/K)$. We begin by considering the case when $\mathcal{G}$ is an abelian p-group.

LEMMA 10: *Assume that $\mathcal{G}$ is an abelian p-group. Then* $\mathrm{Br}(E/K)_{\mathrm{un}} \subseteq \mathcal{C}(E/K)$.

Proof: By Lemma 1, it suffices to prove that each basic element in $\mathrm{Br}(E/K)_{\mathrm{un}}$ is in $\mathcal{C}(E/K)$. Let α be a basic element of order p^r in $\mathrm{Br}(E/K)_{\mathrm{un}}$ and let π_1 and π_2 be the primes of K at which α has non-zero Hasse invariant. Since $\alpha \in \mathrm{Br}(E/K)_{\mathrm{un}}$, π_1 and π_2 are unramified in E. Let δ_i be an extension to E of π_i for $i = 1, 2$. $\mathrm{Gal}(E_{\delta_i}/K_{\pi_i})$ is cyclic and, since E splits α, p^r divides $|\,\mathrm{Gal}(E_{\delta_i}/K_{\pi_i})|$ for $i = 1, 2$. Let σ_i be an element of $\mathrm{Gal}(E_{\delta_i}/K_{\pi_i})$ of order p^r for $i = 1, 2$.

Arguing exactly as in the proof of Theorem 9, we may assume that $\mathcal{G} = \langle \sigma_1, \sigma_2 \rangle$. Since $\mathcal{G}$ has exponent p^r, $\mathrm{Gal}(E_{\delta_i}/K_{\pi_i})$ is cyclic, and $\sigma_i \in \mathrm{Gal}(E_{\delta_i}/K_{\pi_i})$, it follows that $\mathrm{Gal}(E_{\delta_i}/K_{\pi_i}) = \langle \sigma_i \rangle$ for $i = 1, 2$. By Lemma 8, we may assume that $\mathcal{G} \neq \langle \sigma_1 \rangle \times \langle \sigma_2 \rangle$ and so $|\mathcal{G}| < p^{2r}$.

Since σ_1 has maximal order in $\mathcal{G}$, there exists $\sigma_3 \in \mathcal{G}$ such that $\mathcal{G} = \langle \sigma_1 \rangle \times \langle \sigma_3 \rangle$. Assume that $|\langle \sigma_3 \rangle| = p^w$. Then $|\mathcal{G}| = p^{r+w} < p^{2r}$ so $w < r$. Since $\mathcal{G}/\langle \sigma_1 \rangle$ is generated by $\sigma_2 \langle \sigma_1 \rangle$, w is the minimal t such that $\sigma_2^{p^t} \in \langle \sigma_1 \rangle$. Replacing σ_1 and σ_3 by appropriate powers, if necessary, we may suppose that $\sigma_2 = \sigma_1^{p^u} \sigma_3^{p^v}$ for some u, v with $0 \leq u \leq r$ and $0 \leq v \leq w$. We claim that $u = v = 0$. Suppose first that $v \geq 1$. Then $\sigma_2^{p^{w-1}} = \sigma_1^{p^{u+w-1}} \sigma_3^{p^{v+w-1}} = \sigma_1^{p^{u+w-1}} (\sigma_3^{p^w})^{p^{v-1}} = \sigma_1^{p^{u+w-1}} \in \langle \sigma_1 \rangle$, contradicting $p^w = |\mathcal{G}/\langle \sigma_1 \rangle|$. Thus $v = 0$. Now suppose $u \geq 1$. Then $\sigma_2^{p^{r-1}} = \sigma_1^{p^{u+r-1}} \sigma_3^{p^{r-1}} = (\sigma_1^{p^r})^{p^{u-1}} \sigma_3^{p^{r-1}} = \sigma_3^{p^{r-1}}$. Since $w \leq r - 1$, $\sigma_3^{p^{r-1}} = 1_{\mathcal{G}}$ and so $\sigma_2^{p^{r-1}} = 1_{\mathcal{G}}$, contradicting our choice of σ_2 as having order p^r. Thus $\sigma_2 = \sigma_1 \sigma_3$.

Let $L = E^{\sigma_3}$. Since L/K is a cyclic layer of E/K, it suffices to show that L splits α. Fix i with $1 \leq i \leq 2$. Since $\langle \sigma_i \rangle \subseteq \mathrm{Gal}(E_{\delta_i}/K_{\pi_i}) \subseteq \mathrm{Gal}(E/K) = \langle \sigma_1, \sigma_2 \rangle$ and since $\mathrm{Gal}(E_{\delta_i}/K_{\pi_i})$ is cyclic, it follows that $\langle \sigma_i \rangle = \mathrm{Gal}(E_{\delta_i}/K_{\pi_i})$. Let Z_i denote the decomposition field of π_i in L. Since $\mathcal{G}$ is abelian, π_i splits completely in both Z_i and E^{σ_i} and so also in $Z_i E^{\sigma_i}$. But every extension of π_i to E^{σ_i} is undecomposed in E and so $Z_i \subseteq E^{\sigma_i}$. Since $\langle \sigma_3, \sigma_1 \rangle = \langle \sigma_3, \sigma_2 \rangle$, $L \cap E^{\sigma_i} = K$. Since $Z_i \subseteq L$, it follows that $Z_i = K$. But then π_i is undecomposed in L and so π_i has a unique extension γ_i to L. Since $[L_{\gamma_i}: K_{\pi_i}] = [L: K] = p^r$, L splits α. ∎

THEOREM 11: *Let E be a finite Galois extension of the global field K. Let p be a prime and suppose that each Sylow p-subgroup of* $\mathrm{Gal}(E/K)$ *is either abelian or of exponent p. Then* $\mathrm{Br}(E/K)_{\mathrm{un}} \subseteq \mathcal{C}(E/K)$.

Proof: By Proposition 7 and Lemma 10, we may assume that $\mathrm{Gal}(E/K)$ is a p-group of exponent p. By Proposition 3(3), $\mathrm{Br}(E/K)_{\mathrm{un}}$ has exponent p. Theorem 11 now follows from Theorem 9. ∎

As noted previously, there exist examples where $\mathcal{G}$ is an abelian p-group and $\mathrm{Br}(E/K) \neq \mathcal{C}(E/K)$. Such examples can not, however, exist if E is everywhere unramified over K. As an immediate corollary of Theorem 11, we have:

COROLLARY 12: *Let E be a finite Galois everywhere unramified extension of the global field K. Assume that each Sylow subgroup of* $\mathrm{Gal}(E/K)$ *is either abelian* *or of prime exponent. Then* $\mathrm{Br}(E/K) = \mathcal{C}(E/K)$.

Given any finite group $\mathcal{H}$, by the theorem of Scholz-Fröhlich-Uchida [Sc, Satz 6] (or [F]), there exist algebraic number fields $E \supseteq K$ with E Galois and everywhere unramified over K and with $\mathrm{Gal}(E/K) \cong \mathcal{H}$. Assume then that $\mathcal{G}$ is isomorphic to the quaternion group of order 8 and that E is everywhere unramified over K. We will prove that $\mathrm{Br}(E/K) \neq \mathcal{C}(E/K)$, showing that some restriction on the structure of the Sylow subgroups of $\mathrm{Gal}(E/K)$ is necessary in Corollary 12. We begin with a technical lemma.

LEMMA 13: *Assume that $\mathcal{G}$ is isomorphic to the quaternion group of order 8 and that E is an everywhere unramified extension of K. Let $\sigma \in \mathcal{G}$ have order 4. For $\alpha \in \mathrm{Br}(E/K)$, let $\mathcal{S}(\alpha)$ denote the set of primes π of K such that both $\mathrm{l.\,i.}_\pi(\alpha) = 4$ and π has some extension to E which has σ as Frobenius automorphism. If $\alpha \in \mathrm{Br}(E/K)$ with $|\mathcal{S}(\alpha)|$ odd, then $|\mathcal{S}(\alpha + \mathrm{cor}_K^F(\beta))|$ is also odd for every cyclic layer L/F of E/K and every basic element $\beta \in \mathrm{Br}(L/F)$.*

Proof: Let $\alpha \in \mathrm{Br}(E/K)$ with $|\mathcal{S}(\alpha)|$ odd, let L/F be a cyclic layer of E/K, let $\beta \in \mathrm{Br}(L/F)$ be a basic element, and let $\gamma = \mathrm{cor}_K^F(\beta)$. Let $\tilde{\theta}_1$ and $\tilde{\theta}_2$ be the primes of F at which β has non-zero Hasse invariant and let θ_i denote the restriction of $\tilde{\theta}_i$ to K for $i = 1, 2$. If $\theta_1 = \theta_2$, then $\gamma = 0$ since $\mathrm{inv}_{\tilde{\theta}_1}(\beta) = -\mathrm{inv}_{\tilde{\theta}_2}(\beta)$. Thus we may assume that $\theta_1 \neq \theta_2$. Then $\mathrm{inv}_{\theta_i}(\gamma) = \mathrm{inv}_{\tilde{\theta}_i}(\beta)$ for $i = 1, 2$, and $\mathrm{l.\,i.}_{\theta_1}(\gamma) = \mathrm{l.\,i.}_{\theta_2}(\gamma)$. Let π be a prime of K. Since E is everywhere unramified over K, $\mathrm{l.\,i.}_\pi(\alpha) \leq 4$ and $\mathrm{l.\,i.}_\pi(\gamma) \leq 4$ by Proposition 3(3). Thus $\mathrm{inv}_\pi(\alpha), \mathrm{inv}_\pi(\gamma) \in \{0, 1/2, 1/4, 3/4\}$, $\mathrm{inv}_\pi(\alpha + \gamma) = \mathrm{inv}_\pi(\alpha)$ if $\pi \notin \{\theta_1, \theta_2\}$, and $\mathrm{inv}_\pi(\alpha + \gamma) = \mathrm{inv}_\pi(\alpha) + \mathrm{inv}_\pi(\gamma)$ if $\pi \in \{\theta_1, \theta_2\}$. In particular, if $\mathrm{l.\,i.}_{\theta_1}(\gamma) < 4$, then $\mathcal{S}(\alpha) = \mathcal{S}(\alpha + \gamma)$ and so we may assume that $\mathrm{l.\,i.}_{\theta_i}(\gamma) = 4$ for $i = 1, 2$. It follows that $\exp(\beta) = 4$ and so L/F is a cyclic layer of E/K of degree divisible by 4. Since $\mathcal{G}$ is isomorphic to the quaternion group of order 8, $\mathcal{G}$ has no homomorphic images which are cyclic of order 4 and so $L = E$ and $[E\colon F] = 4$. If neither θ_1 nor θ_2 has an extension to E having σ as Frobenius automorphism, then clearly $\mathcal{S}(\alpha) = \mathcal{S}(\alpha + \gamma)$ and so we may assume that θ_1 has an extension to E having σ as Frobenius automorphism. We will show that this forces θ_2 to also have an extension to E having σ as Frobenius automorphism.

Since E splits β, $\tilde{\theta}_i$ is undecomposed in E for $i = 1, 2$. In particular, since σ is the Frobenius automorphism for some extension of θ_1 to E, $\langle\sigma\rangle \subseteq \mathrm{Gal}(E/F)$. It follows that $\mathrm{Gal}(E/F) = \langle\sigma\rangle$. Let τ be the Frobenius automorphism of some extension δ of θ_2 to E. Then τ also has order 4. Suppose that τ is not conjugate to σ. Since σ and σ^3 are conjugate in $\mathcal{G}$, τ is also not conjugate to σ^3. Thus τ is not conjugate to any element of $\langle\sigma\rangle$ and so left multiplication by τ acts as a transposition on the cosets of $\langle\sigma\rangle$ in $\mathcal{G}$. By [J, Proposition 2.8, page 101], θ_2 is undecomposed in F. Since $\tilde{\theta}_2$ is undecomposed in E, it follows that θ_2 is undecomposed in E and so $[E_\delta\colon K_{\theta_2}] = 8 = |\mathcal{G}|$. Thus $\mathrm{Gal}(E_\delta/K_{\theta_2}) = \mathcal{G}$. But $\mathrm{Gal}(E_\delta/K_{\theta_2})$ is cyclic since E is everywhere unramified over K and so $\mathcal{G}$ is cyclic, a contradiction. This shows that θ_2 also has an extension to E having σ as Frobenius automorphism.

Let π be a prime of K having an extension to E having σ as Frobenius automorphism so $\pi \in \mathcal{S}(\alpha+\gamma)$ if and only if $\mathrm{l.i.}_\pi(\alpha+\gamma) = 4$. If $\pi \notin \{\theta_1,\theta_2\}$, then $\mathrm{inv}_\pi(\alpha+\gamma) = \mathrm{inv}_\pi(\alpha)$ and so $\pi \in \mathcal{S}(\alpha+\gamma)$ if and only if $\mathrm{l.i.}_\pi(\alpha) = 4$. If $\pi \in \{\theta_1,\theta_2\}$, then $\mathrm{inv}_\pi(\alpha+\gamma) = \mathrm{inv}_\pi(\alpha) + \mathrm{inv}_\pi(\gamma)$ and so $\pi \in \mathcal{S}(\alpha+\gamma)$ if and only if $\mathrm{l.i.}_\pi(\alpha) \le 2$. A routine verification shows that $|\mathcal{S}(\alpha+\gamma)| \in \{|\mathcal{S}(\alpha)|-2, |\mathcal{S}(\alpha)|, |\mathcal{S}(\alpha)|+2\}$ and so is odd. ∎

PROPOSITION 14: *Let E be a finite Galois everywhere unramified extension of the global field K. Assume that* $\mathrm{Gal}(E/K)$ *is isomorphic to the quaternion group of order 8. Then* $\mathrm{Br}(E/K) \neq \mathcal{C}(E/K)$.

Proof: Let $\mathcal{G} = \mathrm{Gal}(E/K) = \langle\sigma_1,\sigma_2\rangle$. Then σ_1 and σ_2 have order 4 and are not conjugate in $\mathcal{G}$. Fix i with $1 \le i \le 2$. By the Tchebotarev Density Theorem [J, Theorem 10.4] there exists a prime δ_i of E having σ_i as Frobenius automorphism. Let π_i denote the restriction of δ_i to K. Let $\alpha \in \mathrm{Br}(K)$ be the basic element of $\mathrm{Br}(K)$ of order 4 having non-zero Hasse invariants at π_1 and π_2. Then $\alpha \in \mathrm{Br}(E/K)$ since every extension of π_i to E has local degree 4 for $i = 1,2$. Suppose that $\alpha \in \mathcal{C}(E/K)$. Then there exists a set $L_1/F_1,\dots,L_r/F_r$ of cyclic layers of E/K and $\beta_i \in \mathrm{Br}(L_i/F_i)$ such that $\alpha = \sum_{i=1}^r \mathrm{cor}_K^{F_i}(\beta_i)$. By Lemma 1, we may assume that each β_i is basic. Let $\gamma_i = -\mathrm{cor}_K^{F_i}(\beta_i)$. Then $\alpha + \sum_{i=1}^r \gamma_i = 0$. Set $\alpha_0 = \alpha$ and $\alpha_j = \alpha + \sum_{i=1}^j \gamma_i$ for $1 \le j \le r$. Let $\sigma = \sigma_1$ and let $\mathcal{S}(\alpha_j)$ denote the set of primes π of K such that both $\mathrm{l.i.}_\pi(\alpha_j) = 4$ and π has some extension to E which has σ as Frobenius automorphism. By definition of α, $\mathcal{S}(\alpha_0) = \{\sigma_1\}$ since σ_2 is not conjugate to σ_1. Proceeding by induction on j, it follows from Lemma 13 that $|\mathcal{S}(\alpha_j)|$ is odd for $0 \le j \le r$. In particular, $\alpha_r \neq 0$, contradicting $\alpha + \sum_{i=1}^r \gamma_i = 0$. ∎

We remark that a similar result holds if $\mathrm{Gal}(E/K)$ is isomorphic to the wreath product of the cyclic group of order 3 with itself. The proof is similar to that of Proposition 14. We conclude with the promised example showing that the converses of the assertions in Proposition 7, (1) and (2), do not, in general, hold.

PROPOSITION 15: *Let $\mathcal{H} = \langle\sigma, \tau\rangle$ be the quaternion group of order 8 and let $\mathcal{G}$ be the semi-direct product of $\mathcal{H}$ with the cyclic group of order 3 generated by γ where γ permutes σ, τ, and $\sigma\tau$ transitively. Let E be a finite Galois everywhere unramified extension of the global field K and assume that* $\mathrm{Gal}(E/K)$ *is isomorphic to $\mathcal{G}$. Let $M = E^{\mathcal{H}}$. Then* $\mathrm{Br}(E/K)_2 = \mathcal{C}(E/K)_2$ *but* $\mathrm{Br}(E/M)_2 \neq \mathcal{C}(E/M)_2$.

Proof: $\mathrm{Br}(E/M)_2 \neq \mathcal{C}(E/M)_2$ by Proposition 14. Let α be a basic element of $\mathrm{Br}(E/K)_2$ and let π_1 and π_2 be the primes of K where α has non-zero Hasse invariant. By Proposition 3(3), $\exp(\alpha)$ divides the exponent of $\mathcal{G}$ so $\exp(\alpha) = 2$ or 4. If $\exp(\alpha) = 2$, then $\alpha \in \mathcal{C}(E/K)_2$ by Theorem 9 so we may assume that $\exp(\alpha) = 4$. Let δ_1 and δ_2 be, respectively, extensions of π_1 and π_2, respectively, to E. Since E/K is everywhere unramified, $\mathrm{Gal}(E_{\delta_i}/K_{\pi_i})$ is a cyclic subgroup of $\mathcal{G}$ for $i = 1, 2$. Since E splits α, 4 divides $[E_{\delta_i}\colon K_{\pi_i}]$ and so $\mathrm{Gal}(E_{\delta_i}/K_{\pi_i}) = \langle\sigma_i\rangle$ for some $\sigma_i \in \mathcal{H}$ of order 4. But all elements of order 4 in $\mathcal{H}$ are conjugate in $\mathcal{G}$. By Proposition 4, $\alpha \in \mathcal{C}(E/K)$. Since α is an arbitrary basic element of $\mathrm{Br}(E/K)_2$, $\mathrm{Br}(E/K)_2 = \mathcal{C}(E/K)_2$ by Lemma 1. ∎

References

[CF] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory,* Thompson, Washington, D.C., 1967.

[F] A. Fröhlich, *On non-ramified extensions with prescribed Galois group,* Mathematica **9** (1962), 133–134.

[FS] B. Fein and M. Schacher, *A conjecture about relative Brauer groups,* in *K-Theory and Algebraic Geometry: Connections with Quadratic Forms and Division Algebras* (B. Jacob and A. Rosenberg, eds.), Proceedings of Symposia in Pure Mathematics, Vol. 58, Part II, American Mathematical Society, Providence, RI, 1995, pp. 161–169.

[FKS] B. Fein, W. M. Kantor and M. Schacher, *Relative Brauer groups, II,* Journal für die reine und angewandte Mathematik **328** (1981), 39–57.

[J] G. Janusz, *Algebraic Number Fields,* Academic Press, New York, 1973.

[P] R. Pierce, *Associative Algebras*, Springer-Verlag, Berlin–Heidelberg–New York, 1982.

[S] M. Schacher, *Subfields of division rings, I*, Journal of Algebra **9** (1968), 451–477.

[Sc] A. Scholz, *Totale Normenreste, die keine Normen sind, als Erzeuger nicht abelischer Körpererweiterungen II*, Journal für die reine und angewandte Mathematik **182** (1940), 217–234.

[W] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.