PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 130, Number 5, Pages 1333–1337
S 0002-9939(01)06286-4
Article electronically published on November 9, 2001

RELATIVE BRAUER GROUPS AND m-TORSION

ELI ALJADEFF AND JACK SONN

(Communicated by David E. Rohrlich)

ABSTRACT. Let K be a field and $Br(K)$ its Brauer group. If L/K is a field extension, then the relative Brauer group $Br(L/K)$ is the kernel of the restriction map $res_{L/K} : Br(K) \to Br(L)$. A subgroup of $Br(K)$ is called an algebraic relative Brauer group if it is of the form $Br(L/K)$ for some algebraic extension L/K. In this paper, we consider the m-torsion subgroup $Br_m(K)$ consisting of the elements of $Br(K)$ killed by m, where m is a positive integer, and ask whether it is an algebraic relative Brauer group. The case $K = \mathbb{Q}$ is already interesting: the answer is yes for m squarefree, and we do not know the answer for m arbitrary. A counterexample is given with a two-dimensional local field $K = k((t))$ and $m = 2$.

1. Introduction

Let K be a field and $Br(K)$ its Brauer group. If L/K is a field extension, then the relative Brauer group $Br(L/K)$ is the kernel of the restriction map $res_{L/K}$: $Br(K) \to Br(L)$. Relative Brauer groups have been studied by Fein and Schacher (see e.g. [1, 2, 3].) Every subgroup of $Br(K)$ is a relative Brauer group $Br(L/K)$ for some extension L/K [1], and the question arises as to which subgroups of $Br(K)$ are *algebraic relative Brauer groups*, i.e., of the form $Br(L/K)$ with L/K an algebraic extension. For example, if L/K is a finite extension of number fields, then $Br(L/K)$ is infinite [1], so no finite subgroup of $Br(K)$ is an algebraic relative Brauer group. In this paper, we consider the m-torsion subgroup $Br_m(K)$ consisting of the elements of $Br(K)$ killed by m, where m is a positive integer, and ask when is it an algebraic relative Brauer group. For example, if K is a (p-adic) local field, then $Br(K) \cong \mathbb{Q}/\mathbb{Z}$, so $Br_m(K)$ is an algebraic relative Brauer group for all m. This is not surprising, since this Brauer group is "small." The next natural field to look at is a number field, e.g., the rational field $\mathbb{Q}$. Here the situation is somewhat surprising: $Br_m(\mathbb{Q})$ is an algebraic relative Brauer group for all squarefree m, and the question for arbitrary m remains open. In order to construct a counterexample, we take K to be a "two-dimensional local field" $k((t))$ and prove that $Br_2(K)$ is not an algebraic relative Brauer group. We believe that the situation where the m-torsion subgroup of the Brauer group is an algebraic relative Brauer group should be exceptional for general fields.

Received by the editors November 20, 2000.
2000 *Mathematics Subject Classification.* Primary 11R52, 11S25, 12F05, 12G05.
This research was supported by the Fund for the Promotion of Research at the Technion.

2. Reduction

Lemma 2.1. *Let K be a field and $Br(K)$ its Brauer group. Let m_1, m_2 be relatively prime positive integers. Let L_1, L_2 be algebraic extensions of K such that every prime dividing $[L_i : K]$ divides m_i, $i = 1, 2$. (p divides $[L_i : K]$ iff p divides $[F : K]$ for some finite subextension F/K of L_i/K.) Assume that the relative Brauer group $Br(L_i/K)$ equals the m_i-torsion subgroup $Br_{m_i}(K)$, $i = 1, 2$. Then $Br(L_1L_2/K) = Br_{m_1m_2}(K)$.*

Proof. It is clear that $Br(L_1L_2/K) \supseteq Br_{m_1m_2}(K)$. For the opposite inclusion, let $[A] \in Br(L_1L_2/K)$. Then $[A] \in Br(F/K)$ for some finite extension F/K, $F \subset L_1L_2$. Let $F = K(\alpha, \beta, ..., \gamma)$. $\alpha = \sum_i \alpha_i^{(1)} \alpha_i^{(2)}$, $\alpha_i^{(j)} \in L_j$, and similarly for $\beta, ..., \gamma$. Then $F \subseteq E_1E_2$, where $E_j = K(\{\alpha_i^{(j)}, \beta_i^{(j)}, ..., \gamma_i^{(j)}\})$, $E_j \subseteq L_j$, so $[A] \in Br(E_1E_2/K)$, $[E_i : K] = n_i$, where $p|n_i \Rightarrow p|m_i$. In particular, $(n_1, n_2) = 1$. Writing $E = E_1E_2$, we have, noting that $[E : E_1] = n_2$,

$$0 = cor_{E/E_1} res_{E/K}[A] = cor_{E/E_1} res_{E/E_1} res_{E_1/K}[A] = n_2 res_{E_1/K}[A]$$

$$= res_{E_1/K}(n_2[A]) \Longrightarrow n_2[A] \in Br_{m_1}(K).$$

Hence $m_1n_2[A] = 0$. Similarly, $m_2n_1[A] = 0$. Hence $(m_1n_2, m_2n_1)[A] = 0$, and $(m_1n_2, m_2n_1) = d_1d_2$, where $d_i = (m_i, n_i)$, $i = 1, 2$, so $d_1d_2|m_1m_2$, whence $[A] \in Br_{m_1m_2}(K)$. □

Corollary 2.2. *Suppose for each prime p dividing m, p^r is the exact power of p dividing m and there exists an algebraic extension $L^{(p)}/K$ of p-power degree (possibly p^∞) such that $Br_{p^r}(K) = Br(L^{(p)})$. Then $Br_m(K) = Br(L/K)$ with L equal to the composite of the $L^{(p)}$, $p|m$.*

3. m-torsion over $\mathbb{Q}$

Theorem 3.1. *Let l be an odd prime. Let S_0 denote the set of primes p satisfying $p \not\equiv 1 \pmod{l}$, and set $S := S_0 \cup \{l\}$. Define L to be the extension of $\mathbb{Q}$ generated by the lth roots of the elements of S. Then $Br(L/\mathbb{Q}) = Br_l(\mathbb{Q})$.*

Proof. Note that the set S is infinite by Dirichlet's density theorem. Let $\alpha = [A] \in Br_l(\mathbb{Q})$, $E \subset L$, $E/\mathbb{Q}$ finite. We have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Br(E) & \longrightarrow & \bigoplus_p \bigoplus_{\mathfrak{p}|p} Br(E_{\mathfrak{p}}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \\ & & \uparrow res & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & Br(\mathbb{Q}) & \longrightarrow & \bigoplus_p Br(\mathbb{Q}_p) & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array}$$

where the horizontal sequences are the fundamental exact sequences of $Br(\mathbb{Q})$, $Br(E)$, and the middle vertical arrow is for each p, the direct sum of the restriction maps $res_{E_{\mathfrak{p}}/\mathbb{Q}_p}$ for $\mathfrak{p}|p$.

We want to prove that L splits α, so we will show that some finite subextension E of L splits α. If $(\alpha_p)_p$ is the image of α in $\bigoplus_p Br(\mathbb{Q}_p)$, we seek an E such that $E_{\mathfrak{p}}$ splits α_p for all p and all $\mathfrak{p}|p$. Of course we need only consider the finitely many p for which $\alpha_p \neq 0$, hence if we can find, for each such p, a finite extension $E^{(p)} \subset L$ such that $E^{(p)}_{\mathfrak{p}}$ splits α_p for all $\mathfrak{p}|p$, then the composite E of the $E^{(p)}$ will split α.

There are two cases:

Case 1. $p \in S$.

In this case, take $E^{(p)} = \mathbb{Q}(p^{1/l})$ which is contained in L by definition. p is totally ramified of degree l at p, $[E^{(p)}_{\mathfrak{p}} : \mathbb{Q}_p] = l$, hence $E^{(p)}_{\mathfrak{p}}$ splits α_p for every $\mathfrak{p}|p$ (there is only one $\mathfrak{p}|p$ in $E^{(p)}$).

Case 2. $p \notin S$.

It suffices to find a prime $q \in S$ such that $\mathbb{Q}(q^{1/l})$ has local degree l at p. Choose $q \in S$ such that q is a primitive root mod p, by the Chinese remainder theorem and Dirichlet's density theorem. Since $p \notin S$, $p \equiv 1 \pmod l$, so adjoining an lth root of q to $\mathbb{F}_p$ gives an extension of degree p. This insures that p remains prime in $\mathbb{Q}(q^{1/l})$, so taking $E^{(p)} = \mathbb{Q}(q^{1/l})$, we are done in this case, similar to Case 1, since again there is only one prime of $E^{(p)}$ above p. This proves $Br(L/\mathbb{Q}) \supseteq Br_l(\mathbb{Q})$.

In the opposite direction, let $\alpha \in Br(L/\mathbb{Q})$. Then $\alpha \in Br(L'/\mathbb{Q})$ for some finite subextension $L'/\mathbb{Q}$ of $L/\mathbb{Q}$. Since every finite subextension of $L/\mathbb{Q}$ is contained in a finite composite of extensions $\mathbb{Q}(q^{1/l})$, we may assume that L' is such a composite. Observe that $[L' : \mathbb{Q}]$ is a power of l; in fact, it is l^n, where L' is the composite of n of the fields $\mathbb{Q}(q^{1/l})$. (Indeed, if we write $L' = L''(q^{1/l})$ with L'' a smaller composite, then q is totally ramified in $\mathbb{Q}(q^{1/l})$ and unramified in L'', so $L''(q^{1/l})/L''$ is totally ramified at q.) Hence α has order a power of l, by a restriction-corestriction argument. To show $\alpha \in Br_l(\mathbb{Q})$, it suffices to show that α does not have order larger than l, i.e., at most one of the local invariants has order larger than l, for which it suffices to show that for all primes p, with one possible exception $p = l$, $[L'_{\mathfrak{p}} : \mathbb{Q}_p]$ is not divisible by l^2 for at least one $\mathfrak{p}|p$ in L'. In fact, we will show this for *all* $\mathfrak{p}|p$ in L'. For $p = \infty$ this is trivial since l is odd.

Case 1. $p \notin S$. p is unramified in L' so $L'_{\mathfrak{p}}/\mathbb{Q}_p$ is a cyclic extension which is a composite of cyclic unramified extensions of degree $\leq l$, hence of degree dividing the least common multiple of integers $\leq l$, hence not divisible by l^2.

Case 2. $p \in S$, $p \neq l$. Without loss of generality, L' contains $\mathbb{Q}(p^{1/l})$, which is totally ramified of degree l at p. For $q \in S$, $q \neq p$, q is an mth power mod p since $(m, p-1) = 1$ ($q \not\equiv 1 \bmod l$). Hence the polynomial $x^m - q$ has a root in $\mathbb{Q}_p$. It follows that for every $\mathfrak{p}|p$ in L', $L'_{\mathfrak{p}}$ is a composite of $\mathbb{Q}_p(p^{1/l})$ with $\mathbb{Q}_p(\zeta)$, where ζ is some lth root of unity. Hence $[\mathbb{Q}_p(\zeta) : \mathbb{Q}_p]$ divides $l-1$. Therefore, $[L'_{\mathfrak{p}} : \mathbb{Q}_p]$ is not divisible by l^2 for every $\mathfrak{p}|p$ in L'. ☐

By Theorem 3.1 and Corollary 2.2, we have

Corollary 3.2. *If m is an odd squarefree integer, then there exists an algebraic extension L of $\mathbb{Q}$ such that $Br_m(\mathbb{Q}) = Br(L/\mathbb{Q})$.*

We now turn to the case $m = 2$.

Theorem 3.3. *There is a composite L of quadratic extensions of $\mathbb{Q}$ such that $Br_2(\mathbb{Q}) = Br(L/\mathbb{Q})$.*

Proof. Let us call a set S of odd primes *perfect* iff:

$p \equiv 1 \pmod 4$ for every $p \in S$, and

for any two distinct primes $p, q \in S$, p is a quadratic residue modulo q.

There exists a (nonunique) maximal perfect set M (by recursive construction or by Zorn's Lemma). Set $L := \mathbb{Q}(\sqrt{-1}, \{\sqrt{p} | p \in M\})$. We show $Br_2(\mathbb{Q}) = Br(L/\mathbb{Q})$.

Claim. For every prime p (including ∞), $[L_p : \mathbb{Q}_p]$ is even, and is equal to 2 if $p \neq 2$.

Let us first show that the claim implies the result. Consider an element in $Br(L/\mathbb{Q})$. As before, restriction-corestriction implies that the element has 2-power order. It cannot have order bigger than two since $[L_p : \mathbb{Q}_p]$ is bigger than two at only one prime. Conversely, any element of $Br_2(\mathbb{Q})$ is split by L, since it is split by L locally at every prime. □

Proof of the Claim. For $p = \infty$ it is clear since $\sqrt{-1} \in L$. For $p \in M$, $L_p = \mathbb{Q}_p(\sqrt{p})$ since M is perfect. Finally, let $p \notin M$. Then $L_p/\mathbb{Q}_p$ is unramified, hence of degree 1 or 2. If $p \equiv 3 \pmod 4$, then the degree is 2 since $\sqrt{-1} \notin \mathbb{Q}_p$, so assume that $p \equiv 1 \pmod 4$, and contrarily that the degree is 1. Then for every $q \in M$, q is a quadratic residue mod p, which implies, by quadratic reciprocity, that $M \cup \{p\}$ is perfect, contradicting the maximality of M. □

Corollary 3.4. *If m is a positive squarefree integer, then there exists an algebraic extension L of $\mathbb{Q}$ such that $Br_m(\mathbb{Q}) = Br(L/\mathbb{Q})$.*

4. A counterexample

It is conceivable that for any number field K and any m, there exists an algebraic extension L/K such that $Br_m(K) = Br(L/K)$; in any event, we have no counterexample to this for K a number field. We therefore give a counterexample with K a "two-dimensional local field".

Let K be a Laurent series field $k((t))$, where k is any nonarchimedean local field containing $\sqrt{-1}$.[1] We show that there is no algebraic extension L of K such that $Br_2(K) = Br(L/K)$. Suppose L were such an extension. By a theorem of Witt [5, p. 186],

$$Br(K) \cong Br(k) \oplus Hom(G_k, \mathbb{Q}/\mathbb{Z})$$

where G_k denotes the absolute Galois group of k. Extracting 2-torsion,

$$Br_2(K) \cong Br_2(k) \oplus Hom(G_k^{(2)}, \frac{1}{2}\mathbb{Z}/\mathbb{Z})$$

where $G_k^{(2)}$ denotes the maximal elementary abelian 2-quotient of G_k. These are finite groups by local class field theory, hence, without loss of generality, L/K is a finite extension. Let L_1/K denote the maximal subextension of L/K which is unramified (constant) with respect to t. Then $L_1 = \ell_1((t))$, ℓ_1/k finite. We claim $[\ell_1 : k] = 2$. If $[\ell_1 : k] > 2$, L_1 would split a constant algebra (coming from $Br(k)$) of order > 2, hence so would L, contrary to hypothesis. If $[\ell_1 : k] = 1$, then L/K would be totally ramified, $L = k((u))$ (u a local uniformizer for L), and L would not split a constant algebra of order 2.

L/L_1 is totally (and tamely) ramified, so $L = L_1(\sqrt[e]{\pi})$, where π is a local uniformizer of $L_1 = \ell_1((t))$ as above, so $\pi = ct$, $c \in \ell_1^*$. Now $e = [L : L_1]$ is even, for otherwise, $Br_2(K)$ would equal $Br(L_1/K)$. This is impossible as follows: write $\ell_1 = k(\sqrt{a})$ and choose $b \in k^*$ so that a, b are multiplicatively independent in k^*/k^{*2} (such a b exists!). Then L_1 does not split the quaternion algebra (b, t).

Since $e = [L : L_1]$ is even, L contains $L_1(\sqrt{ct}) =: L_2$. Consider the fourth power symbol algebra $(a, t)_4$ over $K = k((t))$. If L splits this algebra which has exponent four, we have a contradiction. Suppose not. By [4, p. 261], $(a, t)_4 \otimes_K L_1$ is Brauer equivalent to the quaternion algebra $(\sqrt{a}, t)$ over L_1. Tensoring this up to L_2 gives

[1] We thank the referee for observing that the above proof holds for k any nonarchimedean local field containing $\sqrt{-1}$; in the original version k was $\mathbb{Q}_p$ with $p \equiv 1 \bmod 4$.

$(\sqrt{a}, t) = (\sqrt{a}, c^{-1}ct) \sim (\sqrt{a}, c^{-1})(\sqrt{a}, ct) \sim (\sqrt{a}, c^{-1})$. By assumption this is not split. $(\sqrt{a}, c^{-1})$ is a constant algebra, defined over ℓ_1. But $Br_2(\ell_1) \cong \mathbb{Z}/2\mathbb{Z}$ (ℓ_1 is a local field). Take an algebra class $[A]$ of exponent four in $Br(k)$. Its restriction to L_1 has exponent two, hence is equivalent to $(\sqrt{a}, c^{-1})$. Let $[A]$ also denote the corresponding (constant) algebra class in $Br(K)$, and set $[B] := [A]^{-1}[(a,t)_4] \in Br(K)$. Then L_2 splits B, whereas $[B]^2 = [A]^{-2}[(a,t)_4]^2 = [A]^{-2}[(a,t)]$ which is not split because the first factor is a constant algebra class of order two and the second is a nonconstant algebra class of order two. Thus $[B]$ is an algebra class of order four in $Br(K)$ which is split by L, contradiction. We conclude $Br_2(K) \neq Br(L/K)$ *for all algebraic extensions* L/K.

References

1. B. Fein and M. Schacher, *Relative Brauer groups I*, J. R. Ang. Math. **321** (1981), 179-194. MR **82f:**12027
2. B. Fein, W. Kantor, and M. Schacher, *Relative Brauer groups II*, J. R. Ang. Math. **328** (1981), 39-57. MR **83a:**12018
3. B. Fein and M. Schacher, *Relative Brauer groups III*, J. R. Ang. Math. **335** (1982), 37-39. MR **83j:**12009
4. I. Reiner, *Maximal Orders*, Academic Press, Orlando, 1975. MR **52:**13910
5. J.-P. Serre, *Local Fields*, Springer-Verlag, New York, 1979. MR **82e:**12016

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

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