HERSHY KISILEVSKY
JACK SONN

On the $n$-torsion subgroup of the Brauer group of a number field

*Journal de Théorie des Nombres de Bordeaux*, tome 15, n° 1 (2003), p. 199-204

[http://www.numdam.org/item?id=JTNB_2003__15_1_199_0]
On the $n$-torsion subgroup of the Brauer group of a number field

par HERSHEY KISILEVSKY et JACK SONN

Résumé. Pour toute extension galoisienne $K$ de $\mathbb{Q}$ et tout entier positif $n$ premier au nombre de classes de $K$, il existe une extension abélienne $L$ de $K$ d’exposant $n$ telle que le $n$-sous-groupe de torsion du groupe de Brauer de $K$ est égal au groupe de Brauer relatif de $L/K$.

Abstract. Given a number field $K$ Galois over the rational field $\mathbb{Q}$, and a positive integer $n$ prime to the class number of $K$, there exists an abelian extension $L/K$ (of exponent $n$) such that the $n$-torsion subgroup of the Brauer group of $K$ is equal to the relative Brauer group of $L/K$.

1. Introduction

Let $K$ be a field, $Br(K)$ 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. [2, 3, 4]). Every subgroup of $Br(K)$ is a relative Brauer group $Br(L/K)$ for some extension $L/K$ [2], 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 [3], so no finite subgroup of $Br(K)$ is an algebraic relative Brauer group. In [1] the question was raised as to whether or not the $n$-torsion subgroup $Br_n(K)$ of the Brauer group $Br(K)$ of a field $K$ is an algebraic relative Brauer group. For example, if $K$ is a ($p$-adic) local field, then $Br(K) \cong \mathbb{Q}/\mathbb{Z}$, so $Br_n(K)$ is an algebraic relative Brauer group for all $n$. This is not surprising, since this Brauer group is “small”. A counterexample was given in [1] for $n = 2$ and $K$ a formal power series field over a local field. Somewhat surprisingly, $Br_2(\mathbb{Q})$ turned out to be an algebraic relative Brauer group.
For number fields \( K \), the problem is a purely arithmetic one, because of the fundamental local-global description of the Brauer group of a number field. In [1], it was proved that \( Br_n(\mathbb{Q}) \) is an algebraic relative Brauer group for all squarefree \( n \). In this paper, we prove the following affirmative result for number fields: given any number field \( K \) Galois over \( \mathbb{Q} \) and any \( n \) prime to the class number of \( K \), \( Br_n(K) \) is an algebraic relative Brauer group, in fact of an abelian extension of \( K \). In particular, \( Br_n(\mathbb{Q}) \) is an algebraic relative Brauer group for all \( n \).

2. Algebraic extensions of \( K \) with local degree \( n \) everywhere

**Theorem 2.1.** Let \( K \) be a number field Galois over \( \mathbb{Q} \) with class number \( h_K \). Let \( \ell \) be a prime number, relatively prime to \( h_K \) and let \( r \) be a positive integer. There exists an abelian extension \( L/K \) of exponent \( \ell^r \) such that the local degree of \( L/K \) at every finite prime equals \( \ell^r \). If \( \ell = 2 \), then \( L \) can be taken to be totally complex.

**Proof.** Let \( k_{\infty} \) be the cyclotomic extension of \( \mathbb{Q} \) obtained by adjoining all \( \ell \)-power roots of unity to \( \mathbb{Q} \). Let \( s \) be a positive integer. For \( \ell \) odd, let \( k_s \) be the unique subfield of \( k_{\infty} \) of degree \( \ell^s \) over \( \mathbb{Q} \). If \( \ell = 2 \), there are three elements of order 2 in \( \text{Gal}(\mathbb{Q}(\mu_{2^{s+1}})/\mathbb{Q}) \), one fixing the maximal real subfield, one fixing \( \mathbb{Q}(\mu_{2^{s+1}}) \), and a third fixing a cyclic totally complex extension of \( \mathbb{Q} \) of degree \( 2^s \), which we define to be \( k_s \). (As usual, \( \mu_m \) denotes the \( m \)th roots of unity.) Then \( \ell \) is the unique prime of \( \mathbb{Q} \) ramified in \( k_s \) and it is totally ramified.

Choose \( s \) such that \( L_0 = Kk_s \) has degree \( \ell^r \) over \( K \). Then the primes \( \ell_1, \ldots, \ell_t \) of \( K \) dividing \( \ell \) have isomorphic completions, and since \( \ell \) is prime to \( h_K \), they are all totally ramified in \( L_0/K \). In the case \( \ell = 2 \), the real primes are also ramified in \( L_0/K \).

Let \( E \) be the extension of \( K \) obtained by adjoining \( L_0 \) and the \( \ell^r \)th roots of all the units of \( K \) (including the \( \ell^r \)th roots of unity). Let \( S \) be the (infinite) set of primes of \( K \) which split completely in \( E \). For \( p \in S \) consider the \( \ell \)-ray class field \( R_p \) with conductor \( p \), i.e. the \( \ell \)-primary part of the ray class field with conductor \( p \). Since the class number \( h_K \) of \( K \) is prime to \( \ell \), \( p \) is totally ramified in \( R_p \). Furthermore, the \( \ell \)-ray class group is isomorphic to the \( \ell \)-part of \( K^* \) modulo the image of the unit group of \( K \). By choice of \( p \in S \), the absolute norm \( N(p) \) is congruent to 1 modulo \( \ell^r \) and all units are \( \ell^r \)th powers in \( K^*_p \). Hence \( K^*_p \) has a (unique cyclic) quotient of order \( \ell^r \). We define \( L^p \) to be the corresponding cyclic subextension of degree \( \ell^r \) of \( R_p \).

Let \( \ell = \ell_1 \) be one of the prime divisors of \( \ell \) in \( K \). Consider the condition \( \ell \) splits completely in \( L^p \) \((p \in S)\). This is equivalent to \( \ell \) being an \( \ell^r \)th
power in the ray class group mod $p$. But since $\ell$ is prime to $h = h_K$, this is equivalent to the principal ideal $\mathfrak{h}^\ell = (a)$, $a \in K^*$, being an $\ell^\ell$th power in the ray class group mod $p$. Since all the units of $K$ are $\ell^\ell$th powers modulo $p$, this is equivalent to $a$ being an $\ell^\ell$th power in $K_p^*$, which for $p \in S$ is equivalent to $p$ splitting completely in $K(\mu_\ell, \sqrt[\ell]{a})$. Denote the $\alpha$ corresponding to $l_i$ by $\alpha_i$.

Let $S' \subset S$ be the set of primes of $K$ that split completely in $E' \subset K(\sqrt[\ell]{a_1}, \ldots, \sqrt[\ell]{a_\ell})$. The prime divisors $l_i$ of $\ell$ in $K$ split completely in $L^p$ if $p \in S'$.

We now define recursively a subsequence $S_0$ of primes of $S'$. We begin with any prime $p_1 \in S'$ such that $\mathcal{N}(p_1) > \mathcal{N}(l_4)$ for $l_4$ dividing $\ell$. (As above, $\mathcal{N}$ denotes the absolute norm.) We claim there exists a prime $p_2 \in S'$ with $\mathcal{N}(p_2) > \mathcal{N}(p_1)$ satisfying:

(a) $p_2$ splits completely in $L^{p_1}$;
(b) $p_1$ splits completely in $L^{p_2}$;
(c) $q$ is inert in $L^{p_2}$ for all primes $q \neq p_1$, $l_i$ of $K$ with absolute norm $\mathcal{N}(q) \leq \mathcal{N}(p_1)$.

To prove the claim, we reduce it to an application of Chebotarev's density theorem. Arguing as above, (b) is equivalent to $p_1$ being an $\ell^\ell$th power in the ray class group mod $p_2$. But since $\ell$ is prime to $h = h_K$, this is equivalent to the principal ideal $p_1^h = (c)$, $c \in K^*$, being an $\ell^\ell$th power in the ray class group mod $p_2$. Since all the units of $K$ are $\ell^\ell$th powers modulo $p_2$, this is equivalent to $c$ being an $\ell^\ell$th power in $K_{p_2}^*$, which is equivalent to $p_2$ splitting completely in $K(\mu_\ell, \sqrt[\ell]{c})$. Thus (b) is a Chebotarev condition compatible with (a).

We now consider (c). We want all $q \neq p_1, l_1, \ldots, l_\ell$ with $\mathcal{N}(q) \leq \mathcal{N}(p_1)$ (these are finitely many) to be inert in $L^{p_2}$. For this it suffices that $q$ be inert in $M^{p_2}$, where $M^{p_2}$ is the subextension of $L^{p_2}$ of degree $\ell$ over $K$. As above, if $q^h = (b)$, $b \in K^*$, this means that (b) is not an $\ell^\ell$th power in the ray class group mod $p_2$, i.e. $b$ is not an $\ell^\ell$th power in $K_{p_2}^*$ (again since all units are $\ell^\ell$th powers in $K_{p_2}^*$), i.e. $p_2$ is nonsplit in $K(\mu_\ell, \sqrt[\ell]{b})$. Since $p_2$ splits in $K(\mu_\ell)$, this is equivalent to $p_2$ being nonsplit in $K(\mu_\ell, \sqrt[\ell]{b})$. For this Chebotarev condition to be compatible with (a) and (b), it suffices that the fields $L^{p_1}E'$ and $K(\mu_\ell, \sqrt[\ell]{b}) : q^h = (b), q \neq p_1, l_i, N(q) \leq N(p_1)$ be linearly disjoint over $K(\mu_\ell)$.

Let $q_1, \ldots, q_u$ be the primes of $K$ distinct from $p_1, l_1, \ldots, l_\ell$ of absolute norm less than or equal to that of $p_1$, and let $q_i^h = (b_i)$, $i = 1, \ldots, u$. Set $K' = K(\mu_\ell)$. We show first that the fields $\{K'(\sqrt[\ell]{b_i}) : i = 1, \ldots, u\}$ are linearly disjoint over $K'$. If not, then by Kummer theory we have an equation $\prod_i b_i^{e_i} = x^\ell$ with $x \in K'$, and not all the $e_i$ divisible by
Taking ideals in $K'$, we have $\prod_{i=1}^{n}(b_i)^{e_i} = (x)^{\ell}$. Since $h_K$ is prime to $\ell$, and the primes $q_i$ are unramified in $K'$, we see that $\ell$ must divide all the $e_i$, contradiction. Set $F_1 := L^{p_1}E'(\sqrt[\ell]{a})$, $F_2 := K'(\sqrt[\ell]{b_1}, \ldots, \sqrt[\ell]{b_n})$. It remains to show that $F_1 \cap F_2 = K'$. If not, then there is a common cyclic subextension $F_3 \subseteq F_1 \cap F_2$ with $[F_3 : K'] = \ell$. On the one hand, $F_3$ is of the form $K'(\sqrt[\ell]{\prod_{i=1}^{n}b_i^{e_i}})$ with not all $e_i$ divisible by $\ell$. For such an $i$, the prime divisors of $q_i$ in $K'$ ramify in $F_3$. But the only primes ramifying in $F_1$ are divisors of $p_1, l_1, \ldots, l_n$, contradiction. Thus the disjointness assertion is proved.

This shows the existence of $p_2$ satisfying (a),(b),(c).

We now assume inductively that $n > 2$ and $p_1, \ldots, p_{n-1} \in S'$ with $\mathcal{N}(p_i) < \mathcal{N}(p_{i+1})$, $i = 1, \ldots, n-2$, have been chosen such that

(a) $p_i$ splits completely in $L^{p_j}$ for all $j < i$, $i = 2, \ldots, n-1$
(b) $p_j$ splits completely in $L^{p_i}$ for all $j < i$, $i = 2, \ldots, n-1$
(c) $q$ is inert in $L^{p_i}$ for all primes $q$ satisfying $\mathcal{N}(p_{i-2}) < \mathcal{N}(q) \leq \mathcal{N}(p_{i-1})$, $q \neq p_{i-1}$, $i = 2, \ldots, n-1$ (take $p_0 = 0$)

(Note and (b) together say $p_i$ splits completely in $L^{p_j}$ for all $i \neq j$, $1 \leq i, j \leq n-1$.)

Claim: There exists a prime $p_n \in S$ satisfying (a),(b),(c).

The argument is similar to that for $p_2$: (a) is satisfied if and only if $p_n$ splits completely in the composite $L^{p_1} \cdots L^{p_{n-1}}$.

(b) is satisfied if $p_n$ splits completely in $K'(\sqrt[\ell]{c_1}, \ldots, \sqrt[\ell]{c_{n-1}})$, where $p_i^{h_i} = (c_i)$, $i = 1, \ldots, n-1$

(c) is satisfied if $p_n$ remains inert in $K'(\sqrt[\ell]{b})$ for each $q^{h} = (b)$, $q \neq p_{n-1}$, with $\mathcal{N}(p_{n-2}) < \mathcal{N}(q) \leq \mathcal{N}(p_{n-1})$. In order to apply the Chebotarev theorem we need the linear disjointness of $L^{p_1} \cdots L^{p_{n-1}} : E'(\sqrt[\ell]{c_1}, \ldots, \sqrt[\ell]{c_{n-1}})$ and the $K'(\sqrt[\ell]{b})$ over $K' = K(\mu_{\ell^r})$, for all the above $b$'s. Since the (c)’s and the (b)’s are distinct prime ideals raised to the power $h$, the previous argument goes through, proving the claim.

We therefore have an infinite sequence $S_0 = \{p_n\}_{n=1}^{\infty}$ of primes of $S'$ satisfying

(i) $p_i$ splits completely in $L^{p_j}$ for all $i \neq j$, and

(ii) $q$ is inert in $L^{p_n}$ for all $q \neq p_{n-1}$ with $\mathcal{N}(p_{n-2}) < \mathcal{N}(q) \leq \mathcal{N}(p_{n-1})$.

Now take $L$ to be the composite of $L_0$ and all the $L^{p_n}$. We check the local degrees of $L/K$:

For $p = p_i \in S_0$, $L$ contains $L^{p_i}$ which is totally ramified of degree $\ell^r$ at $p$. $p$ splits completely in $L_0$, and by (i), $p$ splits completely in $L^{p_j}$ for $j \neq i$, so $[L_p : K_p] = \ell^r$.  


For $p \not\in S_0$, $p$ not dividing $\ell$, $p$ is unramified in $L$, so $L_p/K_p$ is cyclic of exponent dividing $\ell^\epsilon$. There exists a positive integer $n$ such that $N(p_{n-1}) < N(p_n)$. By (ii), $p$ is inert in $L_{p^{n+1}}$ hence $[L_p : K_p] = \ell^\epsilon$. For $p$ dividing $\ell$, $p$ is totally ramified in $L_0$ and splits completely in all the $L^{p_i}$, hence $[L_p : K_p] = \ell^\epsilon$. $L_0$ is totally complex, hence so is $L$. This completes the proof of Theorem 2.1.

Remark 2.2. The hypothesis that $K$ is Galois over $\mathbb{Q}$ guarantees that all primes $4$ dividing $\ell$ in $K$ have isomorphic completions, which is all that is needed in the proof. Also we can have $L/K$ unramified at the infinite primes by choosing the maximal real subfield of $\mathbb{Q}(\zeta_{2n+2})$ in place of $k_s$.

3. The $n$-torsion subgroup of the Brauer group of $K$

Theorem 3.1. Given a number field $K$ Galois over $\mathbb{Q}$ and a positive integer $n$ prime to the class number of $K$, there exists an abelian extension $L/K$ (of exponent $n$) such that the $n$-torsion subgroup of the Brauer group of $K$ is equal to the relative Brauer group of $L/K$.

Proof. Consider the case $n = \ell^\epsilon$, $\ell$ prime. By Theorem 2.1, there exists an abelian $\ell$-extension $L/K$ whose local degree at every finite prime is $\ell^\epsilon$, and is 2 at the real primes if $\ell = 2$. It follows from the fundamental theorem of class field theory on the Brauer group of a number field that $L$ splits every algebra class of order dividing $\ell^\epsilon$, and conversely, any algebra class split by $L$ has order dividing $\ell^\epsilon$. For general $n$, the theorem follows from a straightforward reduction to the prime power case (see [1]).

Remark 3.2. For $K = \mathbb{Q}$, Theorem 3.1 says that $Br_n(\mathbb{Q})$ is an algebraic relative Brauer group for all $n$. The proof of Theorem 2.1 is more concrete in this case because the ray class fields involved are simply the degree $\ell^\epsilon$ subfields of $\mathbb{Q}(\zeta_p)$ with $p \equiv 1 \pmod{\ell^\epsilon}$. Theorem 3.1 was proved in [1] for the case $n$ squarefree, $K = \mathbb{Q}$. The case $n = 2$ was proved there by constructing $L/Q$ with local degree 2 everywhere except perhaps at the prime 2. We are grateful to Romyar Sharifi and David Ford (independently) for a construction of $L/Q$ with local degree 2 everywhere, including 2, the idea of which was instrumental in the proof of Theorem 2.1.

References


Hershy Kisilevsky  
Department of Mathematics  
Concordia University  
11455 de Maisonneuve Blvd. West  
Montreal  
Canada  
*E-mail*: kisilev@mathstat.concordia.ca

Jack Sonn  
Department of Mathematics  
Technion  
32000 Haifa  
Israel  
*E-mail*: sonn@math.technion.ac.il