Journal de Théorie des Nombres de Bordeaux

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, nº 1 (2003), p. 199-204

<http://www.numdam.org/item?id=JTNB_2003__15_1_199_0>

Journal de Théorie des Nombres
de Bordeaux **15** (2003), 199–204

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

par Hershy 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.

Manuscrit reçu le 20 décembre 2001.
The research of the first author was supported in part by grants from NSERC and FCAR. The research of the second author was supported by the Fund for the Promotion of Research at the Technion and the N. Haar and R. Zinn Research Fund.

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 ℓ 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 ℓ^r such that the local degree of L/K at every finite prime equals ℓ^r. If $\ell = 2$, then L can be taken to be totally complex.*

Proof. Let k_∞ be the cyclotomic extension of $\mathbb{Q}$ obtained by adjoining all ℓ-power roots of unity to $\mathbb{Q}$. Let s be a positive integer. For ℓ odd, let k_s be the unique subfield of k_∞ of degree ℓ^s over $\mathbb{Q}$. If $\ell = 2$, there are three elements of order 2 in $\mathrm{Gal}(\mathbb{Q}(\mu_{2^{s+2}})/\mathbb{Q})$, 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, μ_m denotes the mth roots of unity.) Then ℓ 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 ℓ^r over K. Then the primes $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ of K dividing ℓ have isomorphic completions, and since ℓ 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 ℓ^rth roots of all the units of K (including the ℓ^rth roots of unity). Let S be the (infinite) set of primes of K which split completely in E. For $\mathfrak{p} \in S$ consider the ℓ-ray class field $R_\mathfrak{p}$ with conductor $\mathfrak{p}$, *i.e.* the ℓ-primary part of the ray class field with conductor $\mathfrak{p}$. Since the class number h_K of K is prime to ℓ, $\mathfrak{p}$ is totally ramified in $R_\mathfrak{p}$. Furthermore, the ℓ-ray class group is isomorphic to the ℓ-part of $\overline{K}_\mathfrak{p}^* = (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^*$ (the multiplicative group of the residue field) modulo the image of the unit group of K. By choice of $\mathfrak{p} \in S$, the absolute norm $\mathcal{N}(\mathfrak{p})$ is congruent to 1 modulo ℓ^r and all units are ℓ^rth powers in $\overline{K}_\mathfrak{p}^*$. Hence $\overline{K}_\mathfrak{p}^*$ has a (unique cyclic) quotient of order ℓ^r. We define $L^\mathfrak{p}$ to be the corresponding cyclic subextension of degree ℓ^r of $R_\mathfrak{p}$.

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

Let $S' \subset S$ be the set of primes of K that split completely in $E' = E(\sqrt[\ell^r]{a_1}, \dots, \sqrt[\ell^r]{a_t})$. The prime divisors $\mathfrak{l}_i$ of ℓ in K split completely in $L^{\mathfrak{p}}$ if $\mathfrak{p} \in S'$.

We now define recursively a subsequence S_0 of primes of S'. We begin with any prime $\mathfrak{p}_1 \in S'$ such that $\mathcal{N}(\mathfrak{p}_1) > \mathcal{N}(\mathfrak{l}_i)$ for $\mathfrak{l}_i$ dividing ℓ. (As above, $\mathcal{N}$ denotes the absolute norm.)

We claim there exists a prime $\mathfrak{p}_2 \in S'$ with $\mathcal{N}(\mathfrak{p}_2) > \mathcal{N}(\mathfrak{p}_1)$ satisfying:

(a) $\mathfrak{p}_2$ splits completely in $L^{\mathfrak{p}_1}$;

(b) $\mathfrak{p}_1$ splits completely in $L^{\mathfrak{p}_2}$;

(c) $\mathfrak{q}$ is inert in $L^{\mathfrak{p}_2}$ for all primes $\mathfrak{q} \neq \mathfrak{p}_1, \mathfrak{l}_i$ of K with absolute norm $\mathcal{N}(\mathfrak{q}) \leq \mathcal{N}(\mathfrak{p}_1)$.

To prove the claim, we reduce it to an application of Chebotarev's density theorem. Arguing as above, (b) is equivalent to $\mathfrak{p}_1$ being an ℓ^rth power in the ray class group mod $\mathfrak{p}_2$. But since ℓ is prime to $h = h_K$, this is equivalent to the principal ideal $\mathfrak{p}_1^h = (c)$, $c \in K^*$, being an ℓ^rth power in the ray class group mod $\mathfrak{p}_2$. Since all the units of K are ℓ^rth powers modulo $\mathfrak{p}_2$, this is equivalent to c being an ℓ^rth power in $\overline{K}_{\mathfrak{p}_2}^*$, which is equivalent to $\mathfrak{p}_2$ splitting completely in $K(\mu_{\ell^r}, \sqrt[\ell^r]{c})$. Thus (b) is a Chebotarev condition compatible with (a).

We now consider (c). We want all $\mathfrak{q} \neq \mathfrak{p}_1, \mathfrak{l}_1, \dots, \mathfrak{l}_t$ with $\mathcal{N}(\mathfrak{q}) \leq \mathcal{N}(\mathfrak{p}_1)$ (these are finitely many) to be inert in $L^{\mathfrak{p}_2}$. For this it suffices that $\mathfrak{q}$ be inert in $M^{\mathfrak{p}_2}$, where $M^{\mathfrak{p}_2}$ is the subextension of $L^{\mathfrak{p}_2}$ of degree ℓ over K. As above, if $\mathfrak{q}^h = (b)$, $b \in K^*$, this means that (b) is not an ℓth power in the ray class group mod $\mathfrak{p}_2$, *i.e.* b is not an ℓth power in $\overline{K}_{\mathfrak{p}_2}^*$ (again since all units are ℓ^rth powers in $\overline{K}_{\mathfrak{p}_2}^*$), *i.e.* $\mathfrak{p}_2$ is nonsplit in $K(\mu_\ell, \sqrt[\ell]{b})$. Since $\mathfrak{p}_2$ splits in $K(\mu_{\ell^r})$, this is equivalent to $\mathfrak{p}_2$ being nonsplit in $K(\mu_{\ell^r}, \sqrt[\ell]{b})$. For this Chebotarev condition to be compatible with (a) and (b), it suffices that the fields $L^{\mathfrak{p}_1}E'$ and $\{K(\mu_{\ell^r}, \sqrt[\ell]{b}) : \mathfrak{q}^h = (b), \mathfrak{q} \neq \mathfrak{p}_1, \mathfrak{l}_i, \mathcal{N}(\mathfrak{q}) \leq \mathcal{N}(\mathfrak{p}_1)\}$ be linearly disjoint over $K(\mu_{\ell^r})$.

Let $\mathfrak{q}_1, \dots, \mathfrak{q}_u$ be the primes of K distinct from $\mathfrak{p}_1, \mathfrak{l}_1, \dots \mathfrak{l}_t$ of absolute norm less than or equal to that of $\mathfrak{p}_1$, and let $\mathfrak{q}_i^h = (b_i)$, $i = 1, \dots, u$. Set $K' = K(\mu_{\ell^r})$. We show first that the fields $\{K'(\sqrt[\ell]{b_i}) : i = 1, \dots, u\}$ are linearly disjoint over K'. If not, then by Kummer theory we have an equation $\prod_1^u b_i^{e_i} = x^\ell$ with $x \in K'$, and not all the e_i divisible by

ℓ. Taking ideals in K', we have $\prod_1^u (b_i)^{e_i} = (x)^\ell$. Since h_K is prime to ℓ, and the primes $\mathfrak{q}_i$ are unramified in K', we see that ℓ must divide all the e_i, contradiction. Set $F_1 := L^{\mathfrak{p}_1} E'(\sqrt[\ell^r]{c})$, $F_2 := K'(\sqrt[\ell]{b_1}, \dots, \sqrt[\ell]{b_u})$. 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 $K'(\sqrt[\ell]{\prod_1^u b_i^{e_i}})$ with not all e_i divisible by ℓ. For such an i, the prime divisors of $\mathfrak{q}_i$ in K' ramify in F_3. But the only primes ramifying in F_1 are divisors of $\mathfrak{p}_1, \mathfrak{l}_1, \dots, \mathfrak{l}_t$, contradiction. Thus the disjointness assertion is proved.

This shows the existence of $\mathfrak{p}_2$ satisfying (a),(b),(c).

We now assume inductively that $n > 2$ and $\mathfrak{p}_1, \dots, \mathfrak{p}_{n-1} \in S'$ with $\mathcal{N}(\mathfrak{p}_i) < \mathcal{N}(\mathfrak{p}_{i+1})$, $i = 1, \dots, n-2$, have been chosen such that

(a_i) $\mathfrak{p}_i$ splits completely in $L^{\mathfrak{p}_j}$ for all $j < i$, $i = 2, \dots, n-1$

(b_i) $\mathfrak{p}_j$ splits completely in $L^{\mathfrak{p}_i}$ for all $j < i$, $i = 2, \dots, n-1$

(c_i) $\mathfrak{q}$ is inert in $L^{\mathfrak{p}_i}$ for all primes $\mathfrak{q}$ satisfying $\mathcal{N}(\mathfrak{p}_{i-2}) < \mathcal{N}(\mathfrak{q}) \leq \mathcal{N}(\mathfrak{p}_{i-1})$, $\mathfrak{q} \neq \mathfrak{p}_{i-1}$, $i = 2, \dots, n-1$ (take $\mathfrak{p}_0 = 1$)

(Note (a_i) and (b_i) together say $\mathfrak{p}_i$ splits completely in $L^{\mathfrak{p}_j}$ for all $i \neq j$, $1 \leq i, j \leq n-1$.)

Claim: There exists a prime $\mathfrak{p}_n \in S$ satisfying (a_n),(b_n),(c_n).

The argument is similar to that for $\mathfrak{p}_2$: (a_n) is satisfied if and only if $\mathfrak{p}_n$ splits completely in the composite $L^{\mathfrak{p}_1} \cdots L^{\mathfrak{p}_{n-1}}$.

(b_n) is satisfied if $\mathfrak{p}_n$ splits completely in $K'(\sqrt[\ell^r]{c_1}, \dots, \sqrt[\ell^r]{c_{n-1}})$, where $\mathfrak{p}_i^h = (c_i)$, $i = 1, \dots, n-1$

(c_n) is satisfied if $\mathfrak{p}_n$ remains inert in $K'(\sqrt[\ell]{b})$ for each $\mathfrak{q}^h = (b)$, $\mathfrak{q} \neq \mathfrak{p}_{n-1}$, with $\mathcal{N}(\mathfrak{p}_{n-2}) < \mathcal{N}(\mathfrak{q}) \leq \mathcal{N}(\mathfrak{p}_{n-1})$. In order to apply the Chebotarev theorem we need the linear disjointness of $L^{\mathfrak{p}_1} \cdots L^{\mathfrak{p}_{n-1}} \cdot E'(\sqrt[\ell^r]{c_1}, \dots, \sqrt[\ell^r]{c_{n-1}})$ and the $K'(\sqrt[\ell]{b})$ over $K' = K(\mu_{\ell^r})$, for all the above b's. Since the (c_i)'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 $S_0 = \{\mathfrak{p}_n\}_{n=1}^\infty$ of primes of S' satisfying

(i) $\mathfrak{p}_i$ splits completely in $L^{\mathfrak{p}_j}$ for all $i \neq j$,

and

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

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

For $\mathfrak{p} = \mathfrak{p}_i \in S_0$, L contains $L^{\mathfrak{p}_i}$ which is totally ramified of degree ℓ^r at $\mathfrak{p}$. $\mathfrak{p}$ splits completely in L_0, and by (i), $\mathfrak{p}$ splits completely in $L^{\mathfrak{p}_j}$ for $j \neq i$, so $[L_\mathfrak{p} : K_\mathfrak{p}] = \ell^r$.

For $\mathfrak{p} \notin S_0$, $\mathfrak{p}$ not dividing ℓ, $\mathfrak{p}$ is unramified in L, so $L_\mathfrak{p}/K_\mathfrak{p}$ is cyclic of exponent dividing ℓ^r. There exists a positive integer n such that $\mathcal{N}(\mathfrak{p}_{n-1}) < \mathcal{N}(\mathfrak{p}) \leq \mathcal{N}(\mathfrak{p}_n)$. By (ii), $\mathfrak{p}$ is inert in $L^{\mathfrak{p}_{n+1}}$ hence $[L_\mathfrak{p} : K_\mathfrak{p}] = \ell^r$. For $\mathfrak{p}$ dividing ℓ, $\mathfrak{p}$ is totally ramified in L_0 and splits completely in all the $L^{\mathfrak{p}_i}$, hence $[L_\mathfrak{p} : K_\mathfrak{p}] = \ell^r$. 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 $\mathfrak{l}_i$ dividing ℓ 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 $\mathbb{Q}(\mu_{2^{s+2}})$ 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 $n = \ell^r$, ℓ prime. By Theorem 2.1, there exists an abelian ℓ-extension L/K whose local degree at every finite prime is ℓ^r, 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 ℓ^r, and conversely, any algebra class split by L has order dividing ℓ^r. 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 ℓ^r subfields of $\mathbb{Q}(\mu_p)$ with $p \equiv 1 \pmod{\ell^r}$. Theorem 3.1 was proved in [1] for the case n squarefree, $K = \mathbb{Q}$. The case $n = 2$ was proved there by constructing $L/\mathbb{Q}$ 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 $L/\mathbb{Q}$ with local degree 2 everywhere, including 2, the idea of which was instrumental in the proof of Theorem 2.1.

References

[1] E. Aljadeff, J. Sonn, *Relative Brauer groups and m-torsion.* Proc. Amer. Math. Soc. **130** (2002), 1333–1337.

[2] B. Fein, M. Schacher, *Relative Brauer groups I.* J. Reine Angew. Math. **321** (1981), 179–194.

[3] B. Fein, W. Kantor, M. Schacher, *Relative Brauer groups II.* J. Reine Angew. Math. **328** (1981), 39–57.

[4] B. FEIN, M. SCHACHER, *Relative Brauer groups III.* J. Reine Angew. Math. **335** (1982), 37–39.

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