Hamburger Beiträge zur Mathematik

Nr. 270 / April 2007

Ernst Kleinert

On the Restriction and Corestriction of Algebras over Number Fields

On the Restriction and Corestriction of Algebras over Number Fields

by Ernst Kleinert

1. For every field extension L/K one has a restriction map $res = res_{L/K} : B(K) \longrightarrow B(L)$ of Brauer groups, sending a Brauer class $[A]$ to $[A \otimes_K L]$. (So actually, res is extension of scalars; it is called restriction by virtue of the cohomological description of Brauer groups; cf. [Gr], p.125). The kernel of res is denoted $B(L/K)$ and is called the relative Brauer group of the extension. In the case of global fields $B(L/K)$ has been determined in [FKS]. If L/K is separable, one also has a corestriction map $B(L) \longrightarrow B(K)$, cf. [Ke], § 18. The purpose of the present note is to derive information on the kernel and cokernel of both maps in the number field case by making full use of Hasse's "Main Theorem in the Theory of Algebras".

2. If K is a local field of characteristic 0 one has an isomorphism

$$B(K) \simeq \mathbb{Q} / \mathbb{Z} \tag{2.1}$$

by means of Hasse invariants if K is nonarchimedean. For $K = \mathbb{R}$ the group $B(K)$ is cyclic of order 2 and is identified with the group generated by $1/2 + \mathbb{Z}$ in $\mathbb{Q} / \mathbb{Z}$; clearly $B(\mathbb{C}) = 0$. For global K the above-mentioned Main Theorem consists in an exact sequence

$$1 \longrightarrow B(K) \longrightarrow \oplus_v B(K_v) \longrightarrow \mathbb{Q} / \mathbb{Z} \longrightarrow 0 \tag{2.2}$$

where the sum in the middle runs over all primes of K (finite and infinite). We may think of $B(K_v)$ as identified with $\mathbb{Q} / \mathbb{Z}$ (resp., a subgroup thereof), so that the second arrow in (2.2) is a sum of restrictions (relative to the extensions K_v/K) followed by invariant maps. The third arrow in (2.2) is then simply summation. Of course, the complex primes of K could be omitted in (2.2) but for our purposes it is necessary to carry them along.

(2.3) Lemma. For an extension L/K of number fields there is a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & B(K) & \longrightarrow & \oplus_v B(K_v) & \longrightarrow & \mathbb{Q} / \mathbb{Z} & \longrightarrow & 0 \\ & & \text{res} \downarrow & & \text{Res} \downarrow & & \text{f} \downarrow & & \\ 1 & \longrightarrow & B(L) & \longrightarrow & \oplus_w B(L_w) & \longrightarrow & \mathbb{Q} / \mathbb{Z} & \longrightarrow & 0 \end{array}$$

where Res maps the class $[A]$ of $B(K_v)$ to the element of the sum in the lower row having component $[A \otimes_K L_w]$ for a divisor $w|v$ and 0 elsewhere, and f is multiplication by the field degree $n = |L : K|$.

Proof. The commutativity of the first square follows from the equation

$$(A\otimes_K K_v)\otimes_K L_w \simeq (A\otimes_K L)\otimes_L L_w ,$$

which is a special case of the simple fact that a scalar extension can be realized using arbitrary intermediate steps. In order to prove the commutativity of the second square we make use of the identification of local Brauer groups with (subgroups of) $\mathbb{Q}/\mathbb{Z}$. Recall also that in the nonarchimedean local case the diagram

$$\begin{array}{ccc} B(K_v) & \simeq & \mathbb{Q}/\mathbb{Z} \\ \text{res}\ \downarrow & & \downarrow\ f_{w|v} \\ B(L_w) & \simeq & \mathbb{Q}/\mathbb{Z} \end{array} \qquad (2.4)$$

commutes, where $w|v$ and $f_{w|v}$ is multiplication by the local degree $|L_w : K_v|$, cf. [Re]. An analogous, but trivial diagram can be written down for the infinite primes. Now for the element of $\oplus_v B(K_v)$ having $k/m + \mathbb{Z}$ at the v-component and 0 elsewhere, we obtain (with hopefully self-explanating notation)

$$s\ \mathrm{Res}\ (k/m + \mathbb{Z}) = s\,(|L_w : K_v|\ k/m + \mathbb{Z})_{w|v} = n.\,k/m + \mathbb{Z} = f\,s(k/m + \mathbb{Z})$$

because

$$\sum_{w|v} |L_w : K_v| = n .$$

This proves the lemma.

To the diagram in (2.3) we now apply the snake lemma amd obtain an exact sequence

$$1 \longrightarrow \ker \mathrm{res} \longrightarrow \ker \mathrm{Res} \longrightarrow \ker f \xrightarrow{\delta} \mathrm{cok}\ \mathrm{res} \longrightarrow \mathrm{cok}\ \mathrm{Res} \longrightarrow 0 ,$$

where δ is the connecting homomorphism (note that f is surjective). We first deal with ker Res. Clearly,

$$\ker \mathrm{Res} = \oplus_v \ker \mathrm{Res}_v ,$$

where Res_v denotes the restriction of Res to the v-component. Now $l/m + \mathbb{Z}$ lies in the kernel of Res_v if and only if $|L_w : K_v|\ l/m \in \mathbb{Z}$ for all $w|v$. This shows that $\ker \mathrm{Res}_v$ is generated by $1/t_v + \mathbb{Z}$, where

$$t_v = \gcd \{ |L_w : K_v| , \text{ all } w|v \}.$$

Clearly, ker Res is infinite if and only ker res is, which is indeed the case as is shown in [FKS]. Thus we obtain

(2.5) Corollary. $t_v > 1$ infinitely often.

Note that t_v divides n since the local degrees add up to n. For example, if L/K is of prime degree, it follows that infinitely many primes are fully inert in L. If L/K is Galois, the corollary is an easy consequence of Cebotarev's density theorem.

In [FKS] the infinity of B(L/K) is proved with the aid of a theorem on permutation groups, the proof of which in turn relies on the classification of finite simple groups. As the authors point out, this theorem is actually equivalent to the infinity of B(L/K) (in the usual sense that it is much easier to derive one from the other than to derive it directly). If one could prove 2.5 directly, by standard methods of algebraic number theory, this would also give a proof of the mentioned theorem on permutation groups which is independent of the classification.

Next we determine ker δ . Clearly ker f is generated by $a = 1/n + \mathbb{Z}$. Unravelling the definition of δ , we can choose any finite prime v of K and as preimage of a under s the element having $1/n + \mathbb{Z}$ as v-component and 0 elsewhere. Applying Res, we then obtain $\delta(a)$ as the element having w-component $|L_w : K_v| / n + \mathbb{Z}$ for w|v and 0 elsewhere (this lies in the image of B(L) automatically). We choose v totally decomposed in L/K so that $|L_w : K_v| = 1$ for all w|v and there are n of them (the existence of such v follows from Cebotarev after passing to a Galois extension containing L). We must determine the smallest k such that $k\delta(a)$ comes from B(K) under res; of course we may assume that k divides n. Now if $k\,\delta(a) = \text{res}\,[A]$, then A has v-invariant k/n ; for the other primes v' the v' - invariant $h/m + \mathbb{Z}$ must be such that $|L_{w'} : K_{v'}|\, h/m \in \mathbb{Z}$ for all w'|v', equivalenty $\gcd\{ |L_{w'} : K_{v'}|, w'|v' \}\, h/m \in \mathbb{Z}$. At the same time, the invariants must add up to an integer, that is,

$$k/n \equiv - \sum h/m \mod \mathbb{Z} ,$$

where the sum extends over the primes $\neq v$. In other words, A exists if and only if k/n can be written mod $\mathbb{Z}$ as a $\mathbb{Z}$ – linear combination of the numbers $\gcd\{ |L_{w'} : K_{v'}|, w'|v' \}^{-1}$, $v' \neq v$. The maximal denominator which can be generated in this way is the lcm of these numbers. Therefore, A exists if and only if n/k divides

$$l(L/K): = \mathrm{lcm}_v \{\gcd\{ |L_w : K_v|, w|v\}\}$$

(we may include the exceptional prime v since it doesn't contribute to the lcm). This proves

(2.6) Lemma. The order of ker δ equals $d(L/K): = n / l(L/K)$.

(Note that since all the gcd's divide n so does their lcm.) Assume L/K Galois with group G. Then the local degrees are the orders of the various decomposition groups of the primes of L, and primes dividing the same prime of K have conjugate decomposition groups. So we can write

$$l(L/K) = \mathrm{lcm}\ \{ |D| \}\ , \quad d(L/K) = \gcd\ \{ |G : D| \}\ ,$$

where D runs over the subgroups of G which occur as decomposition groups. It follows from Cebotarev that all cyclic subgroups occur (in fact, infinitely often). Of course, non-cyclic subgroups can be decompositions groups only for ramified primes and therefore can occur at most finitely often; also there are restrictions from the well-known structure of the local Galois groups. I know of no general result providing us with information about the actually occurring decomposition groups.

If G has cyclic Sylow groups, then $d(L/K) = 1$ because in this case all Sylow groups are decomposition groups. I claim that $d(L/K) = 1$ holds "generically", i.e. for extensions L/K of degree n having the full symmetric group S_n as Galois group (of the Galois hull E of L over K). It suffices to show that there are always primes which are completely inert. Using the fact that L is a simple extension of K one can assume that the fixgroup S_{n-1} of L is embedded into S_n as the stabilizer of 1. By Cebotarev, every permutation σ is the Frobenius of some unramified prime u of E, dividing the prime v of K, and by a well-known theorem (cf. [Ja], p.101) the primes of L dividing v correspond to the cycles of the operation of σ on the cosets S_n/S_{n-1}, and their degrees to the lengths of these cycles. Writing

$$S_n \ = \ S_{n-1} \cup (12)\, S_{n-1} \cup \ ..... \ \cup (1n)\, S_{n-1}$$

and taking $\sigma = (12...n)$, one sees that there is but one cycle of length n, which proves our claim. To go to the other extreme, if L/K is a Galois, but noncyclic p-extension with no prime totally ramified (for example, suitable biquadratic extensions), then $l(L/K)$ will be a proper divisor of n.

Summarizing, we state

(2.7) Corollary. The kernel of res fits into an exact sequence

$$1 \longrightarrow \ker \mathrm{res} \longrightarrow \ \oplus_v C(t_v) \ \longrightarrow \ C(d(L/K)) \ \longrightarrow \ 1$$

where $C(t)$ denotes a cyclic group of order t.

The description of ker res in [FKS] is more detailed but requires much more work. To bring out the connection, let us assume for simplicity that L/K is Galois. The sequence in (2.7) is the sum of corresponding sequences for the p-parts of the occurring groups (p a rational prime). Let p^m be the maximal order of p-elements of $G = Gal(L/K)$ and let t be an element having this order. By Cebotarev, the elements t, t^p, .. all occur infinitely often as Frobenius automorphisms of unramified primes of L. This produces infinitely many copies of

$$C(p^m) \oplus C(p^{m-1}) \oplus \ldots \oplus C(p)$$

in the p-part of the middle sum of (2.7), and this the typical "infinite part" of ker res as given in [FKS].

In order to obtain a similar result for the cokernel we need the cokernel of Res. Concentrating on the v-block of $\oplus_w B(L_w)$ (the elements having nonzero components at most at the divisors of w) we see that the image of Res_v in this block consists of all vectors $(|L_w : K_v| \; k/m + \mathbb{Z})_{w|v}$. This subgroup is the kernel of the following map $\mathbb{Q}/\mathbb{Z}^{\,s} \longrightarrow \mathbb{Q}/\mathbb{Z}^{s-1}$, where $s = s(v)$ denotes the number of divisors of v : denote these divisors $w(1), \ldots, w(s)$. Now multiply the $w(i)$-component of a vector $(a_w)_w$ by the product of the degrees $|L_w : K_v|$, where $w \neq w(i)$, call that vector $(b_w)_w$ and send it to the vector $(b_{w(1)} - b_{w(s)}, \ldots, b_{w(s-1)} - b_{w(s)})$. (The proof is elementary.) Thus, the cokernel of Res on the v-block is (in the nonarchimedean case) isomorphic to the sum of $s(v)-1$ copies of $\mathbb{Q}/\mathbb{Z}$. For the archimedean primes, one obtains a finite elementary 2-group whose rank depends on the number of real primes of K and the number of their real extensions to L. Summarizing, we state

(2.8) Corollary. The cokernel of res fits into an exact sequence

$$1 \longrightarrow C(l(L/K)) \longrightarrow \text{cok res} \longrightarrow E \oplus (\oplus_v (\mathbb{Q}/\mathbb{Z})^{s(v)-1}) \longrightarrow 0,$$

where v runs over the nonarchimedean primes of K and E is a finite elementary 2-group. In particular, cok res is infinite.

The last statement follows from the fact that infinitely often $s(v) > 1$ (otherwise $L = K$ by a theorem of Bauer).

3. The corestriction can be treated analogously; the results are even simpler (and perhaps less interesting) in spite of the fact that the corestriction is much more difficult to define; we shall need only two functorial properties of it. First we need the analogue of (2.4) in the nonarchimedean local case. Consider the diagram

$$
\begin{array}{ccccc}
 & & B(L) & \simeq & \mathbb{Q}/\mathbb{Z} \\
(3.1) & \text{cor} & \downarrow & & \downarrow \quad g \\
 & & B(K) & \simeq & \mathbb{Q}/\mathbb{Z}
\end{array}
$$

where g is the map which makes the diagram commute. In order to determine g, we use the formula cor res $[A] = [A]^n$ for $[A] \in B(K)$, cf. [Ke], p. 62. For the invariants, this becomes $g\, f(x) = nx$. Since $f(x) = nx$, we see that g is the identity on elements of the form nx , and since $\mathbb{Q}/\mathbb{Z}$ is divisible, we have $g = id$. It follows (perhaps somewhat unexpectedly) that cor is an isomorphism. In the archimedean local case (after the necessary modifications of the right column of (2.9) g becomes identity if $L = K = \mathbb{R}$ and the zero map in the other cases. The analogue of (2.3) is

(3.2) Lemma. For an extension L/K of number fields there is an exact commutative diagram

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & B(L) & \longrightarrow & \oplus_w B(L_w) & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \\
 & & \text{cor}\downarrow & & \text{Cor}\downarrow & & \downarrow \text{id} & & \\
1 & \longrightarrow & B(K) & \longrightarrow & \oplus_v B(K_v) & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0\,,
\end{array}
$$

where Cor sends the vectors in the v-block of $\oplus_w B(L_w)$ to the sum of their components, located at the v-position of $\oplus_v B(K_v)$.

Proof. The commutativity of the left square amounts to the formula

$$\text{inv}_v(\text{cor}\,[B]) = \sum_{w|v} \text{inv}_w [B], \quad [B] \in B(L)\,,$$

which in turn is the paraphrase in terms of algebras of the formula (16) on p.187 of [Ta]. The commutativity of the right square is trivial.

This time the snake lemma leads to isomorphisms

$$\ker \text{cor} \simeq \ker \text{Cor}, \quad \text{cok cor} \simeq \text{cok Cor}\,.$$

Since Cor is obviously surjective, we conclude

(3.3) Corollary. The corestriction map $B(L) \longrightarrow B(K)$ is surjective.

The determination of the kernel is equally easy since for any abelian group A the kernel of the summation map $A^n \longrightarrow A$ is isomorphic to A^{n-1}. Invoking once more the fact that infinitely often $s(v) > 1$, we see

(3.4) Corollary. The kernel of cor is the sum of infinitely many copies of $\mathbb{Q} / \mathbb{Z}$ and a finite elementary 2-group.

References

[FKS] B.Fein/W.M.Kantor/M.Schacher, Relative Brauer Groups II, Journ.Reine u.Angew.Mathem. 328 (1981), 39-57.

[Ja] G.Janusz, Algebraic Number Fields, Academic Press 1973

[Ke] I.Kersten,. Brauergruppen von Körpern, Braunschweig 1990

[Re] I.Reiner, Maximal Orders, Academic Press

[Gr] K.Gruenberg, Profinite Groups, in: Cassels/Fröhlich, Algebraic Number Theory (Brighton Conference), Academic Press 1967

[Ta] J.Tate, Global Class Field Theory, in Cassels/Fröhlich, Algebraic Number Theory (Brighton Conference), Academic Press 1967