Relative Brauer groups. II

By *Burton Fein**) at Corvallis, *William M. Kantor**) at Eugene and *Murray Schacher**) at Los Angeles

§ 1. Introduction

Let $L \supset K$ be fields and let $B(L/K)$, the relative Brauer group of L/K, denote the subgroup of the Brauer group $B(K)$ of K consisting of those Brauer classes of finite dimensional central simple K-algebras which are split by L. In this paper we continue the investigation of the structure of $B(L/K)$ begun in [10].

Let $L \supset K$ be global fields and let p be a prime dividing $[L:K]$. (By a global field we mean either an algebraic number field or an algebraic function field in one variable over a finite field.) As shown in the proof of [10], Proposition 4, the p-primary component $B(L/K)_p$ of $B(L/K)$ is infinite if L is Galois over K. Example 1 of [10] shows, however, that this need not hold if L is not Galois over K. This raises the following natural question: do there exist global fields $L \supset K$, $L \neq K$, with $B(L/K)$ finite? We show in § 3 that the existence of such fields is equivalent to the existence of a finite transitive permutation group G acting on a set Ω, $|\Omega| > 1$, with the property that all nontrivial elements of G of prime power order have fixed points on Ω. Under the assumption that the classification of the finite simple groups is complete, we sketch a proof in § 2 that no such pair (G, Ω) exists.

In § 3 we determine the precise structure of $B(L/K)_p$ for $L \supset K$ global fields. In this case $B(L/K)_p$ has the form $\oplus_\omega [Z(p^n) \oplus Z(p^{n-1}) \oplus \cdots \oplus Z(p)] \oplus H_p$ where H_p is finite; here $Z(m)$ denotes the cyclic group of order m, ω denotes the cardinality of the natural numbers, and $\oplus_\alpha G$ denotes the direct sum of α copies of the group G. This leads us to define an abelian torsion group G to be of relative Brauer type if G satisfies the following conditions:

(1) $|G| = \omega$,

(2) $G_p = \{0\}$ for all but finitely many primes p, and

(3) for each prime p there is an integer $n = n(p) \geqq 0$ such that

$$G_p \cong \oplus_\omega [Z(p^n) \oplus Z(p^{n-1}) \oplus \cdots \oplus Z(p)] \oplus H_p$$

where H_p is finite.

*) This material is based upon work supported by the National Science Foundation under Grant Numbers B. Fein, MCS 79 — 00698, W. M. Kantor, MCS 79 — 03130, M. Schacher, MCS 78 — 27582.

0075-4102/81/0328-0005$02.00

If $L \supset K$ are global fields, then $B(L/K)$ is of relative Brauer type. We investigate the converse question in § 3: which groups of relative Brauer type are isomorphic to $B(L/K)$ for some global fields $L \supset K$?

Let G be a group of relative Brauer type. We prove in § 3 that $G \cong B(L/K)$ for algebraic number fields $L \supset K$ if and only if there exists a finite transitive permutation group having certain special properties determined by G. These group theoretic considerations enable us to show that certain classes of groups of relative Brauer type are, in fact, relative Brauer groups for number fields; in particular, Example 1 of [10] is generalized to yield examples where $B(L/K)_p$ is any preassigned finite abelian p-group.

We turn in § 4 to the question of whether $B(L/K)$ can be finite for $L \supset K$, $L \neq K$, K finitely generated over a global field, and L finite over K. Suppose L is Galois over K and a Sylow p-subgroup of the Galois group $\mathrm{Gal}(L/K)$ of L/K has exponent p^n. We prove, under these hypotheses, that $B(L/K)_p$ has a direct summand isomorphic to $\oplus_\omega[Z(p^n) \oplus Z(p^{n-1}) \oplus \cdots \oplus Z(p)]$. This result is in marked contrast to the theorem of Roquette's [21], Corollary XVIa, that $B(L/K)$ can be $\{0\}$ for K an elliptic function field over a local field and L a cyclic constant field extension. We conclude by raising several natural questions that arise from this investigation.

We will use freely in what follows standard results from the classical theory of central simple algebras and the classification theory of such algebras over global fields by Hasse invariants; we refer the reader to [9] or [20] for expositions of the relevant theory assumed. In § 2 we will also assume that the reader is familiar with various properties of the finite simple groups; we refer the reader to [12] for a general discussion of these groups.

We will, for the most part, maintain the notation and terminology of [10]. By "algebra" we shall always mean "finite dimensional algebra". If A and B are central simple algebras over a field K we write $A \sim B$ to indicate that A is similar to B; the equivalence class of A in $B(K)$ is represented by $[A]$. We will write Brauer groups additively; thus $[A]+[B]=[A \otimes_K B]$. If L is a cyclic extension of K with $\mathrm{Gal}(L/K)=\langle\sigma\rangle$ and $a \in K-\{0\}$, we let $(L/K, \sigma, a)$ denote the usual cyclic algebra generated over L by an element u with $u^n=a$ and $ul=\sigma(l)u$ for $l \in L$ [20], § 30. For K a global field and π a prime of K, we denote the completion of K at π by K_π. For $[A] \in B(K)$, we denote the Hasse invariant of $[A]$ at π by $\mathrm{inv}_\pi[A]$. The index of $A \otimes_K K_\pi$ will be referred to as the local index of $[A]$ at π. p will always denote a rational prime. If $n=p^b r$ where $p \nmid r$, we set $n_p=p^b$ and write $v_p(n)=b$. We denote the characteristic of a field K by $\mathrm{char}\, K$. If $L \supset K$ are fields, we let $\mathrm{t.d.}\, L/K$ denote the transcendence degree of L over K. For L finite over K, we let $N_{L/K}$ denote the norm map from L to K. We have already defined

$$\oplus_\omega[Z(p^n) \oplus Z(p^{n-1}) \oplus \cdots \oplus Z(p)];$$

we adopt the convention that this expression equals $\{0\}$ if $n=0$. If G is a group acting on a set Ω, we let $\mathrm{Orb}_G(\alpha)$ denote the orbit under G of $\alpha \in \Omega$. By a p-element of G we mean an element of order a power of p. In general the notation $H \subset G$ means H is contained in G and may be equal to G; we use $H \subsetneq G$ to say the containment is proper. Finally, if L is a finite extension of K, we denote by $\mathrm{Res}_{L/K}$ and $\mathrm{Cor}_{L/K}$ the restriction and corestriction maps of cohomology theory; we refer the reader to [4], pages 254—257, for the relevant properties of these maps. Additional notation will be introduced as needed.

§ 2. Group theoretic preliminaries

In this section, we will sketch a proof of the following result.

Theorem 1. *Let G be a finite group acting transitively on a set Ω with $|\Omega| > 1$. Then there exists a prime r and an r-element $g \in G$ such that g acts without fixed points on Ω.*

In proving this result we make the basic assumption that the classification of the finite simple group is complete. More precisely, consider the following families: 1. the groups of prime order, 2. the alternating groups A_n, $n \geqq 5$, 3. the groups of Lie type (any characteristic), and 4. the 26 sporadic groups. We refer the reader to [12] (see also [5]) for a discussion of these groups and their properties. With this notation, our standing assumption amounts to the following:

Hypothesis. *Every finite simple group is one of the above.*

Our proof of Theorem 1 is unpleasant. We reduce quickly to the case where G is a finite simple group acting primitively on Ω. Invoking the classification of the finite simple groups, we proceed to eliminate potential counterexamples to the theorem by a tedious case by case verification. It is unfortunate and perhaps even outrageous that our proof of Theorem 1 requires all of this machinery; it would be desirable to have a direct proof of this result. We will not treat each case in complete detail; such a procedure would be repetitious, unenlightening, and would lengthen the paper considerably. We will, instead, give complete arguments for several of the most typical cases and we will indicate the general procedure to be followed in the remaining cases.

Finally, the reader should bear in mind that, with hypotheses as in Theorem 1, there need not exist any $g \in G$ of prime order acting without fixed points on Ω. Consider, for example, the group G consisting of all affine transformations of $GF(p^2)$ of the form $x \to ax+b$, $a \in GF(p^2)-\{0\}$, $b \in GF(p^2)$, where p is a Mersenne prime. Let H be the subgroup of G consisting of these transformations where $a, b \in GF(p)$. Let Ω be the left cosets of H in G and let G act on Ω by translation. It is easy to verify that every element of prime order in G has a fixed point on Ω. There are, however, 2-elements in G which act without fixed points.

Sketch of proof of Theorem 1. Assume that the theorem is false and let (G, Ω) be a minimal counterexample. Then G must act faithfully and transitively on Ω and every element of G of prime power order has fixed points on Ω. Let H be the stabilizer of a point of Ω. Then H satisfies the following condition:

$(*)$ for each prime r, each r-element of G is conjugate to an element of H.

In view of $(*)$ we may assume that H is a maximal subgroup of G. Consequently, if $\{1\} \neq N \lhd G$, then $G = HN$ so that N is transitive on Ω. Since every element of N of prime power order has fixed points on Ω, $N = G$ by our minimality assumption. Thus G is a simple group. Since G is clearly non-abelian, our Hypothesis implies that G is one of the following types: (1) A_n, $n \geqq 5$, (2) Chevalley or twisted of characteristic p, or (3) sporadic. The various cases are handled separately.

Case 1. $G=A_n$, $n\geqq 5$. Let $Y=\{1, 2, \ldots, n\}$ and let G act on Y. We show first that H must be transitive on Y. Suppose not. Then Y can be partitioned into subsets of lengths k and $n-k$ respectively where $1\leqq k<n$ and where each orbit of Y under H lies in one or the other of these subsets. In particular, $H\subset (S_k\times S_{n-k})\cap A_n$. By the maximality of H, $H=(S_k\times S_{n-k})\cap A_n$. Let p be a prime dividing n and let $n=n_p t$. For p odd, let $g\in A_n$ be the product of t disjoint cycles each of length n_p. By $(*)$, H contains a conjugate of g. In particular, $n_p|k$. Similarly, if $p=2$ and $n_2>2$, H contains an element which is the product of $2t$ disjoint cycles each of length $\frac{n_2}{2}$, and so $\frac{n_2}{2}\Big|k$. Thus, for n odd $n|k$, and for n even, $\frac{n}{2}\Big|k$. It follows that n must be even and $k=\frac{n}{2}$. Thus $H=\left(S_{\frac{n}{2}}\times S_{\frac{n}{2}}\right)\cap A_n$ and so $|H|\Big|\left[\left(\frac{n}{2}\right)!\right]^2$. By Bertrand's Postulate [27] (or [13], Theorem 418) there is a prime p satisfying $\frac{n}{2}<p<n$. But then A_n contains elements of order p while H can not contain any such element. This contradicts $(*)$ and so H must be transitive on Y.

We see from $(*)$ that H contains a 3-cycle. By [14], Satz 4. 5, Page 171, H must act imprimitively on Y. By [14], Satz 1. 2, Page 145, there exist m and k with $m>1$, $k>1$, and $n=mk$, such that $|H|$ divides $(m!)\,(k!)^m$. Using Bertrand's Postulate again, we take p prime with $\frac{n}{2}<p<n$. Since $m\leqq\frac{n}{2}$, $k\leqq\frac{n}{2}$, we obtain a contradiction to $(*)$ exactly as above. This finishes Case 1.

Before turning to Chevalley and twisted groups, we recall a theorem of Zsigmondy [30]. Let $q>1$ be a power of a prime p and let $k\geqq 1$. A prime r is called a *primitive divisor* of q^k-1 provided $r|(q^k-1)$ but $r\nmid p^j-1$ whenever $1<p^j<q^k$. Zsigmondy's theorem asserts that q^k-1 has a primitive divisor except in the following cases: (1) $q=2$ and $k=6$, and (2) q is a Mersenne prime and $k=2$.

Case 2. $G=PSL(2, q)$, $q\geqq 4$. We note first that $q\neq 4$, 5, or 9 by Case 1 [14], Chapter 2, § 8. Let $q=p^f$. The possibilities for H are restricted by the fact that H is a maximal subgroup of $PSL(2, q)$ containing elements of order p and of order r for every prime r dividing q^2-1. An examination of the list of subgroups of $PSL(2, q)$ (see [14] Satz 8. 27, p. 213) shows there are four possibilities for maximal subgroups containing elements of order p. These are:

(1) $[G:H]=q+1$ and H is the normalizer of a Sylow p-subgroup;

(2) $H=PSL(2, q')$ or $PGL(2, q')$ with $GF(q')\subsetneqq GF(q)$;

(3) H is dihedral of order $2(q\pm 1)$ and $p=2$; or

(4) H is S_5 or A_5 and $p=3$.

Since G has elements of prime power order >2 dividing either $q-1$ or $q+1$, (1), (3) and (4) cannot occur. In case (2), q cannot be a Mersenne prime, and a primitive divisor of q^2-1 then exists and cannot divide $|H|$.

Case 3. $G=PSL(n, q)$, $n\geqq 3$. By $(*)$, H contains (projective) transvections of the underlying vector space V. Let H^* be the normal subgroup of H generated by all transvections of H.

We temporarily exclude the case $n=6$, $q=2$, and we take r to be a primitive divisor of q^n-1. An element of order r acts irreducibly. If P is a Sylow p-subgroup of H^*, then $H=H^*N_H(P)$ by the Frattini argument. P has fixed points on V spanning a proper subspace, and this space is invariant for $N_H(P)$. Thus $N_H(P)$ cannot act irreducibly, and so $r\nmid|N_H(P)|$. Then $r\,\big|\,|H^*|$ and H^* is irreducible. By [16], Theorem 2, $H^*\subset PSp(n, q)$. Since H contains a cyclic group of prime power order dividing $q^{n-1}-1$ which fixes exactly one 1-space, we have a contradiction.

Similarly, if $G=PSL(6, 2)$, then elements of order 9 and 31 yield the irreducibility of H and H^*, respectively, and we can proceed as before.

Case 4. $G=P\Omega^+(2n, q)$. This is very similar to the preceding case. Define H^* as above using long root elements. Using elements of order dividing q^n-1 and $q^{2n-2}-1$, we find that first H, and then H^*, is irreducible. Primitive divisors can also be used to show that H^* is not contained in an orthogonal group defined over a proper subfield of $GF(q)$. According to [16], this still leaves one possibility: $n=4$ and $H^*=\Omega(7, q)$, with H^* embedded in G via a triality automorphism. But then H fails to meet a suitable conjugacy class of elements of order dividing q^2+1.

Case 5. $G=E_8(q)$. Define H^* as before. Let r be a primitive divisor of $q^{30}-1$. Then r does not divide the order of any parabolic subgroup of G. By [3], r does not divide the order of any p-local subgroup of G. Then $r\,\big|\,|H^*|$ as in Case 3. By [7], (3. 8), H^* is the product of pairwise commuting subgroups, each of which is generated by an H^* conjugacy class of root elements. Thus, since $r\,\big|\,|H^*|$, H^* is generated by such a conjugacy class.

Now [8] applies. A glance reveals that no possibility for H^* listed there has order divisible by r. This eliminates the case $G=E_8(q)$.

Case 6. $G=Sz(q)$. Here we have that $|H|$ is divisible by 2, by a primitive divisor of q^4-1, and by a prime divisor of $q-1$. By [26], § 15, $H=G$.

Case 7. $G={}^2F_4(q)'$. Let B be a Borel subgroup of ${}^2F_4(q)$. Then

$$[{}^2F_4(q):B]=(q^6+1)\,(q^3+1)\,(q^2+1)\,(q+1)$$

is relatively prime to $|B|$. If r is a prime dividing $[{}^2F_4(q):B]$, then a Sylow r-subgroup of ${}^2F_4(q)$ is either cyclic or can be written as the direct product of two non-conjugate cyclic groups. Consequently, $[{}^2F_4(q):B]$ divides $|H|$ by $(*)$. Then ${}^2F_4(q)=BH$, and so $H=G$ by [25].

Remark. The cases of other Chevalley and twisted groups can similarly be reduced to [25]. However, in general, $[G:B]$ and $|B|$ are not relatively prime so that great deal more care is required, in the form of uninteresting subcases and elementary number theory.

Case 8. G is sporadic.

Let Π be the set of primes $r\,\big|\,|G|$ such that if R is a Sylow r-subgroup of G, then $|R|=r$. The largest prime divisor of $|G|$ is in Π (and $N_G(R)$ is a Frobenius group). If G is not the simple group .2 (see [12] for definitions) and if a non-trivial p-group is normalized by an element of order r for all $r\in\Pi$, then $\Pi=\{p\}$.

Let M be a minimal normal subgroup of H. Recall that $|H|$ is divisible by every prime dividing $|G|$. If $G \neq .2$, it follows that M cannot be a p-group for any prime p. Then M is a direct product of isomorphic non-abelian simple groups. Let P be any nontrivial Sylow subgroup of M. Then $H = MN_H(P)$ by the Frattini argument. Since every member of Π divides $|H|$, it follows that some such member r divides $|M|$. Since $r^2 \nmid |G|$, M must be simple. Consequently, we are left with the problem of checking whether G can have a simple subgroup M such that $H = N_G(M)$ satisfies $(*)$. This check will be described in one case: that of the previously excluded group $G = .2$.

Let $G = .2$. There is a unique class of p-subgroups P such that $|G|$ and $|N_G(P)|$ have exactly the same set of prime divisors. Here $|P| = 2^{11}$ and $N_G(P)/P \cong M_{23}$. However, G has two different conjugacy classes of subgroups of order 5, so $5^2 \mid |H|$ by $(*)$. Thus $H \neq N_G(P)$. Proceeding as before, we find that M is simple and non-abelian. Since $C_H(M) \lhd M$, we have $C_H(M) = \{1\}$, so $H \leqq \mathrm{Aut}(M)$.

Since $23 \mid |H|$ but $19 \nmid |H|$, M cannot be an alternating group.

If M is sporadic, a trivial check of orders shows that only M_{23}, M_{24}, and .3 have exactly the same primes dividing their orders as does G. As above, subgroups of order 5 eliminate the first two groups. Similarly, $.3 = \mathrm{Aut}(.3)$ has two classes of involutions, while G has three such classes. Thus $M \neq .3$, and M cannot be sporadic.

Finally, if M is a Chevalley or twisted group of characteristic p, then $p^N \mid |M|$ where N is the number of positive roots. It follows easily that $p = 2$ or 3. Also, $|M|/p^N$ is a product of cyclotomic polynomials evaluated at a power of p, divided by a small greatest common divisor related to the rank of M. Since $2^{11} - 1 = 23 \cdot 89$ and $3^5 - 1 = 2 \cdot 11^2$ while $23 \cdot 11 \mid |G|$, $89 \nmid |G|$ and $11^2 \nmid |G|$, $(*)$ yields a contradiction.

This shows that $G \neq .2$. All the remaining sporadic groups can be eliminated in a very similar manner. It is necessary to use published or unpublished information concerning conjugacy classes and centralizers of elements of prime power order.

This completes our sketch of a proof of Theorem 1.

We conclude this section by constructing an example of a permutation group G on a set Ω such that, for certain prescribed primes q, all q-elements of G have fixed points on Ω. This example will be used in § 3.

Example. Let $q_1, \ldots, q_w$ be a set of rational primes and let $c_1, \ldots, c_w$ be integers with $1 \leqq c_j$ for $j = 1, \ldots, w$. Then there exists a finite group G acting faithfully and transitively on a set Ω such that $q_j^{c_j} \mid |\Omega|$ for $j = 1, \ldots, w$, and such that all q_j-elements of G have fixed points on Ω.

Construction. Let $k < w$. We will construct inductively a group G_k and a subgroup H_k of G_k such that the following conditions are satisfied: (1) H_k does not contain any nontrivial normal subgroup of G_k, (2) $q_j \nmid |G_k|$ for $j > k$, (3) $q_j^{c_j} \mid [G_k : H_k]$ for $j \leqq k$, and (4) for each $j \leqq k$, each q_j-element of G_k fixes a left coset of H_k in G_k.

We begin our induction by setting $G_0 = H_0 = \{1\}$. Let $0 \leqq k < w$ and assume that G_k and H_k have been constructed satisfying conditions (1)—(4) above. We will show how to construct G_{k+1} and H_{k+1}.

Let $q=(q_{n+1})^{c_{n+1}}$, $N=(q-1)\,|G_k|\prod_{j=1}^{k} q_j$, $m=1+\prod_{1\neq p/N} p(p-1)$ and $M=\dfrac{q^m-1}{q-1}$. We claim that $(M, N)=1$. For, if r is a prime dividing (M, N), then the order of q in $GF(r)-\{0\}$ divides both m and $r-1$. Since $m\equiv 1 \pmod{(r-1)}$, we conclude that $q\equiv 1 \pmod r$. Then $M=1+q+\cdots+q^{m-1}\equiv 1+1+\cdots+1=m\equiv 1 \pmod r$, whereas $M\equiv 0 \pmod r$. This proves our claim.

Let $\bar{G}$ denote the group consisting of all affine transformations of $GF(q^m)$ of the form $x\longrightarrow ax+b$, where $a, b\in GF(q^m)$ and $a^M=1$. Let $\bar{H}$ be the subgroup of $\bar{G}$ consisting of those transformations of the form $x\longrightarrow x+b$, $b\in GF(q)$. Set $G_{k+1}=G_k\times\bar{G}$ and $H_{k+1}=H_k\times\bar{H}$. We claim that G_{k+1} and H_{k+1} satisfy conditions (1)—(4).

Before verifying this, we note that the multiplicative group of $GF(q^m)$ is the direct product of its subgroups of order M and $q-1$, since the latter numbers are relatively prime. Consequently, every transformation $x\longrightarrow x+b$, $b\in GF(q^m)$ lies in some $\bar{G}$-conjugate of $\bar{H}$.

We now proceed to verify (1)—(4).

(1) Let $(h, \sigma)\in H_{k+1}$ belong to a normal subgroup of G_{k+1} lying in H_{k+1}; here $h\in H_k$ and $\sigma\in\bar{H}$. Since (1) holds for G_k and H_k, $h=1$. Since the $\bar{G}$-conjugates of $\bar{H}$ cover $GF(q^m)$, $\sigma=1$. Thus (1) holds for G_{k+1} and H_{k+1}.

(2) Note that $|G_{k+1}|=|G_k|q^mM$. If q_j divides $|G_{k+1}|$ for some $j>k+1$, then $q_j|N$ while $(M, N)=1$. Then $q_j\,|\,|G_k|$, whereas (2) holds for G_k and H_k. This proves (2).

(3) follows because $[G_{k+1}: H_{k+1}]=[G_k: H_k]q^{m-1}M$.

(4) Suppose that $j\leqq k+1$ and (g, τ) is a q_j-element of G_{k+1}. Note that $|G_k|$ divides N, $|\bar{G}|$ divides q^mM, and $(qM, N)=1$, (using (2) for G_k to see that $(q, N)=1$). Thus $(|G_k|, |\bar{G}|)=1$, and we see that $\tau=1$ if $j\leqq k$ and $g=1$ if $j=k+1$. Since condition (4) holds for G_k and H_k, we may assume that $j=k+1$. We have already noted that each element of $\bar{G}$ of order q_{k+1} lies in a $\bar{G}$-conjugate of $\bar{H}$. This proves (4), completing the induction.

Now set $G=G_w$ and let Ω be the set of left cosets of H_w in G_w.

§ 3. The structure of $B(L/K)$: the global case

In this section we will study the structure of $B(L/K)$ when $L\supset K$ are global fields. We begin our investigation by determining the structure of the various p-primary components of $B(L/K)$.

Let $L\supset K$ be global fields and let π be a prime of K. We say that π *satisfies* $D(p^i, L)$ if $\min\{v_p([L_\delta: K_\pi])\}=i$ where the minimum is taken over all extensions δ of π to L. We denote the set of primes of K satisfying $D(p^i, L)$ by $N(p^i, L/K)$. With this notation we can now describe $B(L/K)_p$.

Theorem 2. *Let $L \supset K$ be global fields, let p be a fixed prime, and let $m = v_p([L:K])$. There exist integers $n = n(p, L/K) \geqq 0$ and $r(p^i, L/K) \geqq 0$ for $n < i \leqq m$ such that*

$$B(L/K)_p \cong \bigoplus_{\omega} [Z(p^n) \oplus Z(p^{n-1}) \oplus \cdots \oplus Z(p)] \oplus \left[\bigoplus_{i=n+1}^{m} \bigoplus_{r(p^i, L/K)} Z(p^i) \right].$$

The integers $n(p, L/K)$ and $r(p^i, L/K)$ are determined as follows:

(a) *Suppose L is separable over K. Let $L = K(\alpha)$ and let E be a Galois closure of L over K. Then:*

(1) $n(p, L/K) = v_p(\max_{\sigma} \{\min_{\beta} \{|\mathrm{Orb}_{\langle\sigma\rangle}(\beta)|\}\})$

where the minimum is taken over all roots β in E of $\mathrm{Irr}(\alpha, K)$ *and the maximum is taken over all p-elements σ of* $\mathrm{Gal}(E/K)$. *In particular, if L is Galois over K, p^n equals the exponent of a Sylow p-subgroup of* $\mathrm{Gal}(L/K)$.

(2) *Let t be maximal with $N(p^t, L/K) \neq \emptyset$. If $i > t$, then $r(p^i, L/K) = 0$. Assume $t > n(p, L/K)$. If $\pi \in N(p^i, L/K)$ with $n(p, L/K) < i \leqq t$, then π is ramified in L; in particular, $|N(p^i, L/K)| < \infty$ for such i. $r(p^i, L/K) = |N(p^i, L/K)|$ for $n(p, L/K) < i < t$ and*

$$r(p^t, L/K) = |N(p^t, L/K)| - 1.$$

Suppose, moreover, that $\mathrm{char}\, K = q > 0$ *and $p \neq q$. Let p^v equal the exponent of a Sylow p-subgroup of* $\mathrm{Gal}(E/K)$. *Then $r(p^i, L/K) = 0$ if $i > 2v$.*

(b) *Let F denote the separable closure of K in L. If $p \neq \mathrm{char}\, K$, $B(L/K)_p = B(F/K)_p$. Suppose $p = \mathrm{char}\, K$. Let $[L:F] = p^w$. Then $n(p, L/K) = n(p, F/K) + w$ and*

$$r(p^{i+w}, L/K) = r(p^i, F/K) \quad \text{for } n(p, F/K) < i \leqq m.$$

Proof. (a) Assume that L is separable over K, $L = K(\alpha)$, and let E be a Galois closure of L over K. Let π be a prime of K which is unramified in E. Let $\mathrm{Irr}(\alpha, K) = f_1(x) \cdots f_u(x)$ where $f_i(x)$ is a monic irreducible polynomial in $K_\pi[x]$ of degree n_i. Then π has u extensions $\delta_1, \ldots, \delta_r$ to L and $[L_{\delta_i} : K_\pi] = n_i$, $i = 1, \ldots, u$. Now let γ be any extension of π to E and let τ be the Frobenius automorphism of E_γ over K_π. Since $\mathrm{Gal}(E_\gamma/K_\pi)$ is isomorphic to a subgroup of $\mathrm{Gal}(E/K)$ by [29], Proposition 4-10-5, we may assume that $\tau \in \mathrm{Gal}(E/K)$. Since τ generates $\mathrm{Gal}(E_\gamma/K_\pi)$ and since each $f_i(x)$ splits completely in E_γ, $\langle\tau\rangle$ is transitive on the set of roots in E_γ of each of the $f_i(x)$. It follows that τ has cycle type $(n_1, \ldots, n_u)$ viewed as a permutation of the set Ω of roots of $\mathrm{Irr}(\alpha, K)$ in E. Now suppose that π satisfies $D(p^j, L)$. Then $\min\{v_p(n_i) | i = 1, \ldots, u\} = j$. Let τ have order $p^a b$ where $p \nmid b$ and set $\sigma = \tau^b$. Then σ is a p-element of $\mathrm{Gal}(E/K)$ and $v_p(\min_{\beta} \{|\mathrm{Orb}_{\langle\sigma\rangle}(\beta)|\}) = j$ where the minimum is taken over all $\beta \in \Omega$. Conversely, suppose that σ is a p-element of $\mathrm{Gal}(E/K)$ and $j = v_p(\min_{\beta} \{\{|\mathrm{Orb}_{\langle\sigma\rangle}(\beta)|, \beta \in \Omega\}\})$. By the Tchebotarev density theorem [28], Theorem 12, page 289, there is an infinite set of primes of K such that for each prime π in the set, π is unramified in E and σ is the Frobenius automorphism of E_γ over K_π for some extension γ of π to E. By the above argument, π satisfies $D(p^j, L)$. Define $n(p, L/K)$ to be $v_p(\max_{\sigma} \{\min_{\beta} \{|\mathrm{Orb}_{\langle\sigma\rangle}(\beta)|\}\})$ as in the statement of Theorem 2(a). We have shown that $N(p^j, L/K)$ is infinite for $j \leqq n(p, L/K)$ and $N(p^j, L/K)$ is finite, consisting only of primes of K ramified in L, if $j > n(p, L/K)$.

Since $|K|=\omega$, $|B(L/K)_p|\leqq\omega$. By [20], Theorems 28. 5 and 29. 22, $B(L/K)_p$ has no elements of order p^{m+1}. Thus $B(L/K)_p$ is isomorphic to a direct sum of cyclic groups. Let t be maximal with $N(p^t, L/K)\neq\emptyset$. If $[A]\in B(L/K)_p$ has local index p^j at a prime π of K, then $\pi\in N(p^z, L/K)$ for some $z\geqq j$ by [9], Chapter 7, § 5, Satz 2. In particular, $B(L/K)_p$ has exponent at most p^t by [9], Chapter 7, § 5, Satz 6. Let $j\leqq t$. Fix $\pi\in N(p^t, L/K)$. For $\mu\in N(p^j, L/K)$, $\mu\neq\pi$, there exists $[A_\mu]\in B(K)_p$ such that $\mathrm{inv}_\pi[A_\mu]=\frac{1}{p^j}$, $\mathrm{inv}_\mu[A_\mu]=\frac{-1}{p^j}$, and $\mathrm{inv}_\delta[A_\mu]=0$ for all other primes δ of K [9], Chapter 7, § 5, Satz 9. Then $[A_\mu]\in B(L/K)_p$. It is also clear that $B(L/K)_p$ is generated by the various $[A_\mu]$. It follows that

$$B(L/K)_p=\bigoplus_{\omega}[Z(p^n)\oplus Z(p^{n-1})\oplus\cdots\oplus Z(p)]\oplus H_p$$

where $n=n(p, L/K)$ and where H_p is a finite abelian p-group. Express H_p as a direct sum of cyclic p-groups and let $r(p^i, L/K)$ be the number of direct summands isomorphic to $Z(p^i)$. We clearly may assume that $n(p, L/K)<i\leqq t$. By the above argument we have $r(p^i, L/K)=|N(p^i, L/K)|$ for $n(p, L/K)<i<t$ and $r(p^t, L/K)=|N(p^t, L/K)|-1$ if $|N(p^t, L/K)|\geqq 2$. But if $|N(p^t, L/K)|=1$, then $r(p^t, L/K)=0$ by [9], Chapter 7, § 5, Satz 9. Thus $r(p^t, L/K)=|N(p^t, L/K)|-1$. Finally, we note that if L is Galois over K, then L is generated by any root of $\mathrm{Irr}(\alpha, K)$ and so only the identity of $\mathrm{Gal}(L/K)$ fixes an element of Ω. In particular, if σ is a p-element of maximal order in $\mathrm{Gal}(L/K)$, then all orbits of Ω under $\langle\sigma\rangle$ have length equal to the order of σ. It follows that σ has order p^n with $n=n(p, L/K)$.

We have now proved all of part (a) of the Theorem with the exception of the last assertion of (2). Suppose then that $\mathrm{char}(K)=q>0$ and $p\neq q$. Let p^v equal the exponent of a Sylow p-subgroup of $\mathrm{Gal}(E/K)$ and suppose for some $i>2v$, $r(p^i, L/K)\neq 0$. We argue as in the proof of [10], Proposition 5. Suppose $B(L/K)_p$ contains an element $[A]$ of order p^{2v+1}. $[A]$ must have local index p^{2v+1} at some prime π of K. Since $[A]$ is split by L, π satisfies $D(p^j, L)$ for some $j\geqq 2v+1$. Let γ be any extension of π to E and let V be the maximal tamely ramified extension of K_π in E_γ. Since $[E_\gamma: V]=q^r$ for some r, we conclude that p^j divides $[V: K_\pi]$. In particular, p^{2v+1} divides $[V: K_\pi]$. Since V is tamely ramified over K_π, $\mathrm{Gal}(V/K_\pi)$ is metacyclic [29], § 3—6. But then $\mathrm{Gal}(V/K_\pi)$ contains an element of order p^{v+1}. Since $\mathrm{Gal}(V/K_\pi)$ is a homomorphic image of $\mathrm{Gal}(E/K_\pi)\subset\mathrm{Gal}(E/K)$, we conclude that $\mathrm{Gal}(E/K)$ contains an element of order p^{v+1}. This contradiction completes the proof of part (a) of the Theorem.

(b) Suppose next that L is not separable over K and let F be the separable closure of K in L. Then $[L: F]=q^w$ where $q=\mathrm{char}\,K$. If $q\neq p$, $B(L/K)_p=B(F/K)_p$. Suppose $q=p$. Then L splits every element of $B(F)$ of order dividing p^w [23], Corollary, page 244. Let π and μ be primes of K satisfying, respectively, $D(p^t, F)$ and $D(p^j, F)$ where $t\geqq j$. Let $[B_\mu]$ be the element of $B(K)_p$ of order p^j such that

$$\mathrm{inv}_\pi[B_\mu]=\frac{1}{p^{j+w}},\ \mathrm{inv}_\mu[B_\mu]=\frac{-1}{p^{j+w}},\ \text{and } \mathrm{inv}_\delta[B_\mu]=0 \text{ for all other primes } \delta \text{ of } K.$$

Then $[B_\mu\otimes_K F]$ has order p^w in $B(F)$ so $[B_\mu]\in B(L/K)_p$. We now repeat the argument used in proving part (a) using the $[B_\mu]$'s instead of the $[A_\mu]$'s. This proves (b) and completes the proof of Theorem 2.

Corollary 3. *Let L be a finite separable extension of a global field K and let E be a Galois closure of L over K. Let $L=K(\alpha)$ and let Ω be the set of roots in E of* $\mathrm{Irr}(\alpha, K)$. *Then $B(L/K)_p$ is finite if and only if every p-element of* $\mathrm{Gal}(E/K)$ *fixes an element of Ω.*

Proof. $B(L/K)_p$ is finite if and only if, in the notation of Theorem 2, $n(p, L/K)=0$. The Corollary now follows from part (a) of Theorem 2.

An example where $B(L/K)_p$ is finite but non-zero appears in [10], Example 1. There $\mathrm{Gal}(E/K)\cong A_4$ and L is the fixed field under an element of $\mathrm{Gal}(E/K)$ of order 2. By the theorem of Scholz-Fröhlich-Uchida [24], Satz 6 (or [11]), there exists a number field K_0 and a Galois extension E_0 of K_0 with E_0 globally unramified over K_0 and $\mathrm{Gal}(E_0/K_0)\cong A_4$. Taking L_0 again to be the fixed field of an element of $\mathrm{Gal}(E_0/K_0)$ of order 2, we obtain an example of global fields $L_0 \supset K_0$ with $2|[L_0:K_0]$ but $B(L_0/K_0)_2=\{0\}$. The triviality of $B(L_0/K_0)_2$ follows from Theorem 2.

Corollary 4. *Let $L\supset K$ be global fields, $L\neq K$. Then $B(L/K)$ is infinite.*

Proof. By Theorem 2, part (b), we may assume that L is separable over K. Let $L=K(\alpha)$, let E be a Galois closure of L over K, and let Ω be the set of roots of $\mathrm{Irr}(\alpha, K)$ in E. By Corollary 3, $B(L/K)$ is finite if and only if all elements of prime power order in $\mathrm{Gal}(E/K)$ have fixed points on Ω. But this is impossible by Theorem 1.

We note that, in our statement of Corollary 4, we are maintaining the assumption of § 2 that the classification of the finite simple groups is complete. It would, of course, be more satisfying to have a proof of Corollary 4 which does not depend on the classification of the finite simple groups. We point out, however, that it is easy to show that Theorem 1 and Corollary 4 are equivalent; this follows from an application of the theorem of Scholz-Fröhlich-Uchida referred to above. In particular, a more elementary proof of Corollary 4 would also yield a simpler proof of Theorem 1.

Assume, for simplicity, that L is separable over K and let E be a Galois closure of L over K. Let $L=K(\alpha)$. Then the action of $\mathrm{Gal}(E/K)$ on the set of roots in E of $\mathrm{Irr}(\alpha, K)$ is equivalent to the natural action of $\mathrm{Gal}(E/K)$ on the left cosets of $\mathrm{Gal}(E/L)$ in $\mathrm{Gal}(E/K)$. Thus $n(p, L/K)$ is determined purely group-theoretically in terms of $\mathrm{Gal}(E/K)$ and $\mathrm{Gal}(E/L)$. On the other hand, the integers $r(p^i, L/K)$ are determined number-theoretically by the properties of the primes of K which are ramified in L.

We turn next to the question of determining the groups occurring as $B(L/K)$ with $L\supset K$ global fields. It should be clear from the preceding results that this is a very subtle question and is one which is closely tied to difficult group-theoretic considerations. Any result asserting that a particular group G is isomorphic to $B(L/K)$ with $L\supset K$ global fields is equivalent, by Theorem 2, to a result about the existence of global fields with prescribed local behavior. For example, Corollary 4 is equivalent to the assertion that given any global fields $L\supset K$, $L\neq K$, there exists a prime p and a prime π of K unramified in L such that π satisfies $D(p, L)$. In what follows we will restrict our analysis to algebraic number fields; a similar discussion can presumably be given for the function field case. We begin by defining a class of groups which are the natural candidates for groups of the form $B(L/K)$.

We say that a group G *is of relative Brauer type* if G is an abelian torsion group of cardinality ω such that $G_p = \{0\}$ for all but finitely many primes p and such that for each prime p there exists an integer $n = n(p) \geqq 0$ such that

$$G_p \cong \bigoplus_{\omega} [Z(p^n) \oplus Z(p^{n-1}) \oplus \cdots \oplus Z(p)] \oplus H_p,$$

where $|H_p| < \infty$. If $L \supset K$ are global fields, then $B(L/K)$ is of relative Brauer type; this follows from Theorem 2 and Corollary 4. It should be clear from Theorem 2 that if a group G of relative Brauer type is to be isomorphic to $B(L/K)$ for some algebraic number fields $L \supset K$, there must exist a permutation group $\tilde{G}$ on a set Ω having certain special properties determined by the structure of G. Our next definition describes the class of permutation groups that we will need to consider.

Let V be a non-empty finite set of rational primes, $V = \{p_1, \ldots, p_v\}$, and let $a_1, b_1, a_2, b_2, \ldots, a_v, b_v$ be integers with $1 \leqq a_i \leqq b_i$ for $1 \leqq i \leqq v$. Let W be a possibly empty set of rational primes disjoint from V, $W = \{q_1, \ldots, q_w\}$, and let $c_1, \ldots, c_w$ be integers with $1 \leqq c_j$ for $1 \leqq j < w$. Let $\tilde{G}$ be a finite transitive permutation group on a set Ω. We say that $(\tilde{G}, \Omega)$ is of Type B with respect to $\{(p_i, a_i, b_i), (q_j, c_j) | 1 \leqq i \leqq v,\ 1 \leqq j \leqq w\}$ if the following three conditions are satisfied:

(1) $p_i^{b_i} q_j^{c_j} \big| |\Omega|$ for $1 \leqq i \leqq v$, $1 \leqq j \leqq w$,

(2) if $p \big| |\Omega|$, $p \notin V$, then every p-element of $\tilde{G}$ has fixed points on Ω, and

(3) for each i, $1 \leqq i \leqq v$, $v_{p_i}\left(\max_{\sigma} \{\min_{\beta} \{|\mathrm{Orb}_{\langle \sigma \rangle}(\beta)|\}\}\right) = a_i$ where the minimum is taken over all $\beta \in \Omega$ and the maximum is taken over all p_i-elements σ of $\tilde{G}$.

Theorem 5. *Let G be a group of relative Brauer type. Let $V = \{p_1, \ldots, p_v\}$ be the set of primes p such that G_p is infinite, let $a_i = n(p_i)$, and let H_{p_i} have exponent $p_i^{b_i}$. Let $W = \{q_1, \ldots, q_w\}$ be the set of primes p such that G_p is finite but non-zero and let H_{q_j} have exponent $q_j^{c_j}$. Then there exist algebraic number fields $L \supset K$ with $B(L/K) \cong G$ if and only if there exists a finite transitive permutation group $\tilde{G}$ on a set Ω such that $(\tilde{G}, \Omega)$ is of Type* B *with respect to $\{(p_i, a_i, b_i), (q_j, c_j) | 1 \leqq i \leqq v,\ 1 \leqq j \leqq w\}$.*

Proof. If there exists a number field $K(\alpha) \supset K$ with $B(K(\alpha)/K) \cong G$, then it is clear from the preceding results that $(\mathrm{Gal}(E/K), \Omega)$ is of Type B with respect to

$$\{(p_i, a_i, b_i), (q_j, c_j) | 1 \leqq i \leqq v,\ 1 \leqq j \leqq w\}$$

where E is a Galois closure of $K(\alpha)$ over K and Ω is the set of roots of $\mathrm{Irr}(\alpha, K)$ in E. Conversely, assume that there exists $(\tilde{G}, \Omega)$ which is of Type B with respect to $\{(p_i, a_i, b_i), (q_j, c_j) | 1 \leqq i \leqq v,\ 1 \leqq j \leqq w\}$. We will construct algebraic number fields $L \supset K$ with $B(L/K) \cong G$. The construction will involve four steps; for simplicity of notation we will denote the relevant pair of fields constructed at each stage by L and K.

Step 1. In this step we will construct a pair of number fields $L \supset K$ such that $B(L/K)_p$ is infinite if and only if $p \in V$ and such that there are "enough" primes π of K satisfying $D(p^z, L)$ for $p \in V \cup W$, z "large enough". The meaning of the phrases "enough" and "large enough" will become clear as the proof proceeds.

Let $\tilde{G} \subset S_u$, the symmetric group on u symbols, and let d be a large integer to be specified later; d will depend on $\tilde{G}$, Ω, and u. We start by determining a number field F by two applications of the Grunwald-Wang theorem [2], Chapter 10, Theorem 5. (The use of the Grunwald-Wang theorem is not really necessary; we use it only for convenience.) To begin we take F_0 a cyclic extension of $Q(\sqrt{-1})$ of degree d such that if π is a prime of $Q(\sqrt{-1})$ with $\pi|Q=p$ and $p|u!$, then π is unramified of degree d in F_0. We then take F cyclic of degree d over F_0 such that if π is a prime of F_0 and $\pi|Q=p$ with $p|u!$, then π splits completely in F. Let $S(p)$ be a Sylow p-subgroup of S_u. We assume that d has been chosen sufficiently large so that if π is a prime of F with $\pi|Q=p$, $p|u!$, then there exists a totally ramified Galois extension E_γ of F_π with $S(p)\cong \mathrm{Gal}(E_\gamma/F_\pi)$; this is possible by the results of [17], § 10. We now imitate the proof of [22], Theorem 9. 1. By [22], Theorem 8. 3, E_γ is the splitting field over F_π of a monic polynomial $f_\pi(x)\in F_\pi[x]$ of degree u. Using the strong approximation theorem, [29], Proposition 4-1-4, we can construct a sequence $\{f_n(x)\}$ of monic polynomials $f_n(x)\in F[x]$, each of degree u, such that $|f_n(x)-f_\pi(x)|_\pi < 1/n$ for all primes π of F extending a rational prime p with $p|u!$; here $|\ |_\pi$ denotes the valuation in F_π. Let π be as above and let $g_\pi(x)$ be an irreducible factor in $F_\pi[x]$ of $f_\pi(x)$. By the argument on Pages 44—46 of [1], we can choose n large enough so that for every root α_i of $f_\pi(x)$, there is a root $\beta_i^{(n)}$ of $f_n(x)$ belonging to α_i with $\{\beta_i^{(n)}\}\to\alpha_i$; the $\beta_i^{(n)}$ are elements of an algebraic closure of E_γ. Let $\alpha=\alpha_1$ be a root of $g_\pi(x)$ and let $\mathrm{Irr}(\beta_1^{(n)}, F_\pi)=g_n(x)$. Extracting a subsequence of $\{f_n(x)\}$, we may assume that $\{g_n(x)\}$ all have the same degree. Since $\{\beta_i^{(n)}\}\to\alpha_i$, $\{g_n(x)\}\to g_\pi(x)$. Thus

$$[F_\pi(\beta_i^{(n)}):F_\pi]=[F_\pi(\alpha):F_\pi]$$

for n sufficiently large. By Krasner's Lemma [1], Page 44, $F_\pi(\beta_1^{(n)})\supset F_\pi(\alpha)$ and so we conclude that $F_\pi(\beta_1^{(n)})=F_\pi(\alpha)$ for n sufficiently large. It follows that E_γ is the splitting field of $f_n(x)$ over F_π for n sufficiently large.

Choose n sufficiently large so that $f(x)=f_n(x)$ has splitting field E_γ over F_π for all primes π of F with $\pi|Q=p$ where $p|u!$. Let E be the splitting field of $f(x)$ over F. Since $f(x)$ has degree u, $\mathrm{Gal}(E/F)\subset S_u$. Since $\mathrm{Gal}(E_\gamma/F_\pi)\cong S(p)\subset \mathrm{Gal}(E/F)$ for all $p|u!$, we see that $\mathrm{Gal}(E/F)\cong S_u$. Let K be the fixed field of $\tilde{G}$, let $\tilde{H}$ be the stabilizer of a point in Ω, and let L be the fixed field of $\tilde{H}$. By Theorem 2, $B(L/K)_p$ is infinite if and only if $p\in V$.

Let π be a prime of F with $\pi|Q=p$ where $p\in V\cup W$. Since $[K:F]=\sum_\lambda [K_\lambda:F_\pi]$, the sum being taken over all extensions λ of π to K, there exists an extension δ of π to K such that $v_p([K_\delta:F_\pi])\leqq v_p([K:F])$. Let $b=b_i$ if $p=p_i\in V$ and let $b=c_j$ if $p=q_j\in W$. Suppose $v_p([L_\theta:K_\delta])<b$ for some extension θ of δ to L. Let γ be any extension of θ to E. Since $\mathrm{Gal}(E_\gamma/F_\pi)\cong S(p)$, $v_p([E_\gamma:F_\pi])=v_p([E:F])$. Since E is Galois over L, $v_p([E_\gamma:L_\theta])\leqq v_p([E:L])$. Since $p^b\big||\Omega|=[L:K]$, $b\leqq v_p([L:K])$. Thus

$$\begin{aligned} v_p([E:F]) &= v_p([E_\gamma:F_\pi])=v_p([E_\gamma:L_\theta])+v_p([L_\theta:K_\delta])+v_p([K_\delta:F_\pi]) \\ &< v_p([E:L])+b+v_p([K:F])\leqq v_p([E:L])+v_p([L:K])+v_p([K:F])=v_p([E:F]). \end{aligned}$$

We conclude that $v_p([L_\theta:K_\delta])\geqq b$ for all extensions θ of δ to L. In particular, δ satisfies $D(p^z, L)$ for some $z\geqq b$. Since there are at least d primes π of F with $\pi|Q=p\in V\cup W$, we see that there are at least d such δ's as above. This completes Step 1.

Step 2. In this step we will modify F, K, L, and E so as to be able to assume that all primes π of F with $\pi|Q = p \notin V \cup W$ are unramified in E. Let π be a prime of F which is ramified in E and let $p = \pi|Q$. Suppose $p \notin V \cup W$. Let γ be any extension of π to E. Then E_γ is a Galois extension of F_π of degree dividing $u!$. Let $E_\gamma = F_\pi(\alpha_\pi)$ and set $g_\pi(x) = (\mathrm{Irr}(\alpha_\pi, F_\pi))^{k_\pi}$ where $k_\pi = u!/[E_\gamma : F_\pi]$ is such that $g_\pi(x)$ has degree $u!$. Now suppose $p \in V \cup W$. Let $g_\pi(x)$ be a monic irreducible polynomial in $F_\pi[x]$ of degree $u!$ such that any root of $g_\pi(x)$ generates the unramified extension of F_π of degree $u!$ over F_π. Finally, let λ be any prime of F which splits completely in E; the existence of λ is guaranteed by the Tchebotarev density theorem. Let $g_\lambda(x)$ be a monic irreducible polynomial of degree $u!$ in $F_\lambda[x]$ such that any root of $g_\lambda(x)$ generates the unramified extension of F_λ of degree $u!$ over F_λ. We construct $g(x) \in F[x]$ monic of degree $u!$ sufficiently close to $g_\lambda(x)$ in the λ-topology and sufficiently close to $g_\pi(x)$ in the π-topology for all primes π of F ramified in E. Since $g_\lambda(x)$ is irreducible in $F_\lambda[x]$, $g(x)$ is irreducible in $F[x]$. Let $M = F(\beta)$ where β is a root of $g(x)$. We have $M \cap E = F$ since λ splits completely in E but is inertial in M. Thus $\mathrm{Gal}(ME/M) \cong S_u$. Let π be a prime of F ramified in E and let α be any root of $g(x)$ over F_π. Since $g(x)$ is sufficiently close to $g_\pi(x) = (\mathrm{Irr}(\alpha_\pi, F_\pi))^{k_\pi}$, α is close to some root of $\mathrm{Irr}(\alpha_\pi, F_\pi)$. By Krasner's Lemma, $F_\pi(\alpha) \supset F_\pi(\alpha_\pi) = E_\gamma$. It follows that if δ is any extension of π to M, then δ splits completely in ME. It is now clear that the properties established in Step 1 are still preserved if we replace F by M, K by MK, L by ML, and E by ME; in addition, we also have the property that now the only primes of F ramifying in E lie over rational primes in $V \cup W$. By Theorem 2, $B(L/K)_p = 0$ if $p \notin V \cup W$. This completes Step 2.

Step 3. Let $p \in V \cup W$ and express H_p as a direct sum of cyclic groups. Assume that $Z(p^t)$ occurs $r(p^t)$ times in this decomposition; we may assume that $a_i < t \leqq b_i$ if $p = p_i$ and $1 \leqq t \leqq c_j$ if $p = q_j$. Define $s(p^t)$ to be $r(p^t)$ unless $p = p_i$ and $t = b_i$ or $p = q_j$ and $t = c_j$; define $s(p^t)$ to be $r(p^t)+1$ if $p = p_i$ and $t = b_i$ or $p = q_j$ and $t = c_j$. In this step we will modify K, L, and E, preserving the properties established in Steps 1 and 2, so as to ensure that there are sets $M(p^t)$ of primes of K with $|M(p^t)| = s(p^t)$ for $p \in V \cup W$ and such that if $\pi \in M(p^t)$ then π satisfies $D(p^t, L)$.

For $p \in V \cup W$ and t with $s(p^t) \neq 0$, arbitrarily choose a set $M(p^t)$ of primes of K satisfying: (1) $|M(p^t)| = s(p^t)$, (2) if $\pi \in M(p^t)$, then π satisfies $D(p^z, L)$ with $z \geqq t$, and (3) if $\pi \in M(p^t)$, then $\pi|Q = p$. We require also that $M(p^t) \cap M(q^z) = \emptyset$ unless $p = q$ and $t = z$. By Steps 1 and 2, we can choose d sufficiently large so as to guarantee the existence of these sets.

Let $\pi \in M(p^t)$, let γ be any extension of π to E, and let $\Theta = \gamma|L$. By assumption, $v_p([L_\Theta : K_\pi]) \geqq t$. Since $\mathrm{Gal}(E_\gamma/K_\pi)$ is a p-group, there is a subfield T_π of E_γ, $L_\Theta \supset T_\pi \supset K_\pi$, with $[L_\Theta : T_\pi] = p^t$. Let $T_\pi = K_\pi(\beta_\pi)$. Since $[T_\pi : K_\pi]$ divides $u!$, $k_\pi = u!/[T_\pi : K_\pi]$ is an integer. Set $h_\pi(x) = (\mathrm{Irr}(\beta_\pi, K_\pi))^{k_\pi}$ so that $h_\pi(x)$ has degree $u!$. Let λ be any prime of K splitting completely in E and let $h_\lambda(x)$ be a monic irreducible polynomial of degree $u!$ in $K_\lambda[x]$ such that any root of $h_\lambda(x)$ generates the unramified extension of K_λ of degree $u!$. Construct $h(x) \in K[x]$ monic of degree $u!$ sufficiently close to $h_\lambda(x)$ in the λ-topology and sufficiently close to $h_\pi(x)$ in the π-topology for all $\pi \in M(p^t)$ with $s(p^t) \neq 0$. Let β be a root of $h(x)$. Replace K by $K(\beta)$, L by $L(\beta)$, E by $E(\beta)$. For each $\pi \in M(p^t)$, arbitrarily choose one extension of π to $K(\beta)$ which satisfies $D(p^t, L(\beta))$; the set of primes so chosen will be the new $M(p^t)$. As in Step 1 and 2, it is easy to verify that the new choices of K, L, and E have the properties required of them.

Step 4. In this final step we will modify K and L so that $B(L/K) \cong G$. In view of Theorem 2, we need to modify K and L, preserving the properties established in Steps 1—3, so that a prime π of K which is ramified in L satisfies $D(p^t, L)$ with $t > a_i$ if $p = p_i$ or $t \geqq 1$ if $p = q_j$ if and only if $S(p^t) \neq 0$ and $\pi \in M(p^t)$.

Let π be a prime of K which is ramified in L. By Step 2, $\pi|Q \in V \cup W$. Suppose π satisfies $D(p^t, L)$ with $t > a_i$ if $p = p_i$ or $t \geqq 1$ if $p = q_j$. Since $\mathrm{Gal}(E_\gamma/K_\pi)$ is a group of prime power order, the prime being $\pi|Q$, we see that $\pi|Q$ must equal p; here γ is any extension of π to E. Exactly as in Step 2, we construct an irreducible polynomial $f(x) \in F[x]$ of degree $u!$ such that the field $K(\beta)$ generated over K by a root β of $f(x)$ has the following properties: (1) $K(\beta) \cap E = K$, (2) if δ is any extension of π to $K(\beta)$ where π is ramified in L and satisfies $D(p^t, L)$ with $t > a_i$ if $p = p_i$ or $t \geqq 1$ if $p = q_j$, then δ splits completely in $E(\beta)$, and (3) if $\pi \in M(p^t)$ then π is unramified in $K(\beta)$ of local degree $u!$. We replace K by $K(\beta)$ and L by $L(\beta)$; it is clear from the above that the new K and L have the required properties. This completes the proof of Theorem 5.

Corollary 6. *An abelian torsion group G is isomorphic to $B(L/K)$ with $L \supset K$ algebraic number fields where L is Galois over K if and only if G is of relative Brauer type and G_p is infinite for all primes p with $G_p \neq \{0\}$.*

Proof. The necessity is clear from Theorem 2. Conversely, suppose G is of relative Brauer type and also has the property that G_p is infinite whenever $G_p \neq \{0\}$. Let $V = \{p_1, \ldots, p_v\}$ be the set of primes p where $G_p \neq \{0\}$. In the notation of Theorem 5, let $a_i = n(p_i)$ and let H_{p_i} have exponent $p_i^{b_i}$. Let $W = \emptyset$. Let $\tilde{G} = \bigoplus_{i=1}^{v} [\oplus_{b_i} Z(p_i^{a_i})]$ and let $L \supset K$ be algebraic number fields with L Galois over K and $\mathrm{Gal}(L/K) \cong \tilde{G}$. Let $L = K(\alpha)$ and let Ω be the set of roots in L of $\mathrm{Irr}(\alpha, K)$. Then $(\tilde{G}, \Omega)$ is of Type B with respect to $\{(p_i, a_i, b_i) | 1 \leqq i \leqq v\}$. Let $\tilde{H}$ be the stabilizer in $\tilde{G}$ of a point in Ω. Since L is Galois over K, only the identity can fix a point so $\tilde{H} = \{1\}$. From the proof of Theorem 5 we can arrange $E = L$ and $B(L/K) \cong G$.

Corollary 7. *Let H be any finite abelian group. Then there exist algebraic number fields $L \supset K$ such that $B(L/K)_p$ is isomorphic to the Sylow p-subgroup of H for all $p \big| |H|$.*

Proof. Let $q_1, \ldots, q_w$ be the set of primes dividing $|H|$ and let $q_j^{c_j}$ be the exponent of the Sylow q_j-subgroup of H. In view of Theorem 5, we need to construct a finite transitive permutation group $\tilde{G}$ on a set Ω such that $(\tilde{G}, \Omega)$ is of Type B with respect to $\{(p_i, a_i, b_i), (q_j, c_j) | 1 \leqq i \leqq v,\ 1 \leqq j \leqq w\}$ for some set of primes $p_1, \ldots, p_v$ and some integers $a_1, b_1, \ldots, a_v, b_v$. Since the p_i's are irrelevant for our problem, it is clear that we need to construct a finite group $\tilde{G}$ acting faithfully and transitively on a set Ω such that $q_j^{c_j} \big| |\Omega|$ for $j = 1, \ldots, w$, and such that each q_j-element of $\tilde{G}$ has a fixed point on Ω. Such a pair $(\tilde{G}, \Omega)$ is constructed in the Example in § 2.

§ 4. Finitely generated extensions of global fields

Let K be a finitely generated extension of a global field F_0 and L be a finite dimensional Galois extension of K. Let p^n be the exponent of a Sylow p-subgroup of $\mathrm{Gal}(L/K)$. If K happens to be global (that is, K is algebraic over F_0), then, according to Theorem 2, $B(L/K)_p \cong \bigoplus_{\omega} [Z(p^n) \oplus Z(p^{n-1}) \oplus \cdots \oplus Z(p)] \oplus H_p$, where H_p is finite. Our next result gives some information in the case that K is not algebraic over F_0.

Theorem 8. *Let K be a finitely generated extension of a global field and let L be a finite dimensional Galois extension of K. Let p^n be the exponent of a Sylow p-subgroup of* $\mathrm{Gal}(L/K)$. *Then $B(L/K)_p$ has a direct summand isomorphic to*

$$\bigoplus_{\omega} [Z(p^n) \oplus Z(p^{n-1}) \oplus \cdots \oplus Z(p)].$$

Proof. Let $\sigma \in \mathrm{Gal}(L/K)$ have order p^n and let $\tau_i = \sigma^{p^{n-i}}$. Let L_i denote the subfield of L which is the fixed field of $\langle \tau_i \rangle$. Then $L = L_0 \supset L_1 \supset \cdots \supset L_n$ and L is a cyclic extension of L_i of degree p^i with $\mathrm{Gal}(L/L_i) = \langle \tau_i \rangle$. Consider the following statement:

$(*)$ there are sets $T_i \subset L_i - \{0\}$, $i = 1, \ldots, n$, satisfying:

(1) $|T_i| = \omega$ for $i = 1, \ldots, n$,

(2) $\mathrm{Res}_{L_i/K} \mathrm{Cor}_{L_i/K}[(L/L_i, \tau_i, b)]$ has order p^i in $B(L/L_i)$ for all $b \in T_i$ and all $i = 1, \ldots, n$, and

(3) $\{\mathrm{Res}_{L_1/K} \mathrm{Cor}_{L_1/K}[(L/L_1, \tau_1, b)] | b \in T_i, \ i = 1, \ldots, n\}$ is a set of independent elements of $B(L/L_1)$.

We show that the Theorem follows from $(*)$. Assume that $(*)$ has been shown to hold and let G be the subgroup of $B(L/K)$ generated by $\{\mathrm{Cor}_{L_i/K}[(L/L_i, \tau_i, b)] | b \in T_i, \ i = 1, \ldots, n\}$. We will show that G is a direct summand of $B(L/K)$ and that

$$G \cong \bigoplus_{\omega} [Z(p^n) \oplus Z(p^{n-1}) \oplus \cdots \oplus Z(p)].$$

Let $b \in T_i$. Since the order of $[(L/L_i, \tau_i, b)]$ in $B(L/L_i)$ divides the index of $(L/L_i, \tau_i, b)$, $[(L/L_i, \tau_i, b)]$ has order dividing p^i. Since $\mathrm{Res}_{L_i/K}$ and $\mathrm{Cor}_{L_i/K}$ are homomorphisms, we conclude by (2) of $(*)$ that $\mathrm{Cor}_{L_i/K}[(L/L_i, \tau_i, b)]$ has order p^i in $B(L/K)$. Now suppose there is a relation:

$$0 = \sum_j a_j \mathrm{Cor}_{L_{i(j)}/K}[(L/L_{i(j)}, \tau_{i(j)}, b_j)]$$

where $1 \leqq i(j) \leqq n$ for all j and $b_j \in T_{i(j)}$. We may assume that $p^{i(j)} \nmid a_j$ for all j. Multiply this relation by p^r where r is maximal such that $p^{i(j)} \nmid p^r a_j$ for some j. Eliminating terms which have been annihilated by p^r, we may assume that our relation has the form:

$$0 = \sum_j c_j p^{i(j)-1} \mathrm{Cor}_{L_{i(j)}/K}[(L/L_{i(j)}, \tau_{i(j)}, b_j)]$$

where $p \nmid c_j$ for all j. Thus

$$0 = \sum_j c_j \mathrm{Res}_{L_1/K}\left(p^{i(j)-1} \mathrm{Cor}_{L_{i(j)}/K}[(L/L_{i(j)}, \tau_{i(j)}, b_j)]\right).$$

But

$$\begin{aligned}
&\mathrm{Res}_{L_1/K}\left(p^{i(j)-1} \mathrm{Cor}_{L_{i(j)}/K}[(L/L_{i(j)}, \tau_{i(j)}, b_j)]\right) \\
&\quad = \mathrm{Res}_{L_1/K} \mathrm{Cor}_{L_{i(j)}/K}[L_1 : L_{i(j)}] \cdot [(L/L_{i(j)}, \tau_{i(j)}, b_j)] \\
&\quad = \mathrm{Res}_{L_1/K} \mathrm{Cor}_{L_{i(j)}/K} \mathrm{Cor}_{L_1/L_{i(j)}} \mathrm{Res}_{L_1/L_{i(j)}}[(L/L_{i(j)}, \tau_{i(j)}, b_j)] \\
&\quad = \mathrm{Res}_{L_1/K} \mathrm{Cor}_{L_1/K}[(L/L_1, \tau_1, b_j)]
\end{aligned}$$

by [4], pages 255—256, formulas 6 and 8. We conclude that

$$0=\sum_j c_j \operatorname{Res}_{L_1/K} \operatorname{Cor}_{L_1/K}[(L/L_1, \tau_1, b_j)]$$

where $p\nmid c_j$ for all j. This contradicts condition (3) of $(*)$. From condition (1) of $(*)$ we conclude that

$$G=\bigoplus_\omega [Z(p^n)\oplus Z(p^{n-1})\oplus\cdots\oplus Z(p)].$$

Finally, to show that G is a direct summand of $B(L/K)$ we must show that if $p^n x\in G$ with $x\in B(L/K)$ then $p^n x=0$. Suppose $x\in B(L/K)$ with $p^n x\in G-\{0\}$. Express $p^n x$ in terms of the given set of generators of G. As above multiply through by p^r where r is chosen suitably. Then for some $m\geqq n$, $p^m x=\sum_j d_j p^{i(j)-1}\operatorname{Cor}_{L_{i(j)}/K}[(L/L_{i(j)}, \tau_{i(j)}, b_j)]$ where $p\nmid d_j$ for all j and $b_j\in T_{i(j)}$. Applying $\operatorname{Res}_{L_1/K}$ to both sides we obtain:

$$p^m \operatorname{Res}_{L_1/K} x=\sum_j d_j \operatorname{Res}_{L_1/K}\operatorname{Cor}_{L_1/K}[(L/L_1, \tau_1, b_j)].$$

But $\operatorname{Res}_{L_1/K}x\in B(L/L_1)$. Since $[L:L_1]=p$ and $p^m\geqq p^n\geqq p$, $p^m\operatorname{Res}_{L_1/K}x=0$. By condition (3) of $(*)$, $p|d_j$ for all j. This contradiction shows that $(*)$ implies the Theorem.

We now prove $(*)$. Suppose first that K is a global field. Let $Y_i=\{\delta_0|\delta_0$ is a prime of K unramified in L and τ_i is the Frobenius automorphism for some extension of δ_0 to $L\}$. $|Y_i|=\omega$ by the Tchebotarev density theorem. For each $\delta_0\in Y_i$ fix some extension δ of δ_0 to L_i. Then δ_0 splits completely in L_i and δ is inert from L_i to L. Let $Z_i=\{\delta|\delta_0\in Y_i\}$. Fix $\gamma\in Z_i$. For $\delta\in Z_i$, $\delta\neq\gamma$, define $A_\delta\in B(L_i)$ to be the element of $B(L_i)$ such that $\operatorname{inv}_\gamma A_\delta=\frac{1}{p^i}$, $\operatorname{inv}_\delta A_\delta=-\frac{1}{p^i}$, and $\operatorname{inv}_\mu A_\delta=0$ for all primes μ of L_i, $\mu\notin\{\gamma,\delta\}$. Since L splits A_δ, $A_\delta=[(L/L_i, \tau_i, b_\delta)]$ for some $b_\delta\in L_i$. b_δ is determined up to norms from L. For each $\delta\in Z_i$ with $\delta\neq\gamma$ fix some b_δ as above and let T_i be the set of b_δ's as selected. We claim that the various T_i, $i=1,\ldots,n$, satisfy $(*)$. Condition (1) of $(*)$ is clear. By [6], page 187 or [19], page 235, $\operatorname{inv}_{\gamma_0}\operatorname{Cor}_{L_i/K}A_\delta=\frac{1}{p^i}$, $\operatorname{inv}_{\delta_0}\operatorname{Cor}_{L_i/K}A_\delta=-\frac{1}{p^i}$, and $\operatorname{inv}_\theta\operatorname{Cor}_{L_i/K}A_\delta=0$ for all primes θ of K, $\theta\notin\{\delta_0,\gamma_0\}$. Thus $\operatorname{Res}_{L_i/K}\operatorname{Cor}_{L_i/K}A_\delta$ has invariant $1/p^i$ at all primes of L_i lying over γ_0, invariant $-1/p^i$ at all primes of L_i lying over δ_0, and invariant 0 at all other primes of L_i. It follows that condition (2) of $(*)$ holds. Finally, let $b_\delta\in T_i$. Then $[(L/L_1, \tau_1, b_\delta)]=\operatorname{Res}_{L/L_1}A_\delta$. It follows that $[(L/L_1, \tau_1, b_\delta)]$ has invariant $1/p$ at the unique prime of L_1 extending γ, invariant $-1/p$ at the unique prime of L_1 extending δ, and invariant 0 at all other primes of L_1. Thus $\operatorname{Res}_{L_1/K}\operatorname{Cor}_{L_1/K}[(L/L_1, \tau_1, b_\delta)]$ has non-zero invariant at a prime μ of L_1 if and only if μ extends either γ_0 or δ_0. But $Y_i\cap Y_j=\emptyset$ unless $i=j$. The results of [20], § 32, now show that condition (3) of $(*)$ holds.

Suppose now that K is an arbitrary finitely generated extension of a global field F_0 and let $d=$ t.d. K/F_0. We proceed by induction on d. The case $d=0$ has been treated above so we may assume that $d\geqq 1$. By [15], page 166, there is a subfield F of K of transcendence degree $d-1$ over a global subfield of K and an element t of K, t transcendental over F, such that L is a finite separable extension of $F(t)$. Let E be a Galois closure of L over $F(t)$ and let $E=F(t)(\alpha)$. Let $f(x,t)=\operatorname{Irr}(\alpha, F(t))$. We have

$$f(x,t)=x^r+\sum_{i=0}^{r-1} a_i(t)\, b_i(t)^{-1}x^i$$

where $a_i(t)$, $b_i(t) \in F[t]$ and $b_i(t) \neq 0$. By the Hilbert Irreducibility Theorem [18], Theorem 2, page 155, there exists $c \in F$ such that $b_i(c) \neq 0$ for $i=1, \ldots, r-1$, $f(x, c)$ is irreducible in $F[x]$, and if $a_i(t) \neq 0$, then $a_i(c) \neq 0$. Let φ be the discrete rank one valuation of $F(t)$ trivial on F and having $t-c$ as uniformizing parameter. We extend φ to E and denote the extended valuation by φ also. Since $f(x, t)$ is monic and has coefficients in the valuation ring of φ, α is also in the valuation ring of φ. Let $\beta \to \bar{\beta}$ denote the residue class map. Since E is separable over $F(t)$, $\dfrac{\partial f(x, t)}{\partial x} \neq 0$. Since $a_i(c) \neq 0$ if $a_i(t) \neq 0$, and $b_i(c) \neq 0$ for all i, it follows that $\dfrac{\partial f(x, c)}{\partial x} \neq 0$. Thus $f(x, c)$ is a separable irreducible polynomial in $F[x]$ and $\bar{\alpha}$ is a root of $f(x, c)$. Since $f(x, c)$ has degree $[E: F(t)]$,

$$[F(\bar{\alpha}): F] = [E: F(t)]$$

and $F(\bar{\alpha})$ is separable over F. Thus φ is unramified and inertial in E. From valuation theory we conclude that $\bar{L}$ is Galois over $\bar{K}$ and $\mathrm{Gal}(\bar{L}/\bar{K}) \cong \mathrm{Gal}(L/K)$ under the natural isomorphism, $\sigma \to \bar{\sigma}$ and $\tau_i \to \bar{\tau}_i$.

By our inductive hypothesis applied to $\bar{L}/\bar{K}$ there exist sets $\bar{T}_i \subset \bar{L}_i - \{0\}$, $i=1, \ldots, n$, satisfying $(*)$. For each $i=1, \ldots, n$, and each $\bar{b} \in \bar{T}_i$, choose $b \in L_i$ with $b \to \bar{b}$. Let T_i be the set of b's chosen, one for each $\bar{b} \in \bar{T}_i$. We will show that the various T_i's, $i=1, \ldots, n$, satisfy $(*)$. Condition (1) of $(*)$ is satisfied since $|\bar{T}_i| = \omega$. We must verify conditions (2) and (3).

Consider the following statement:

$(**)$ if d is an element of the valuation ring of L_1 with $\bar{d} \neq 0$ and if

$$\mathrm{Res}_{\bar{L}_1/\bar{K}} \mathrm{Cor}_{\bar{L}_1/\bar{K}_1} [(\bar{L}/\bar{L}_1, \bar{\tau}_1, \bar{d})] \neq 0,$$

then $\mathrm{Res}_{L_1/K} \mathrm{Cor}_{L_1/K} [(L/L_1, \tau_1, d)] \neq 0$.

Assume that we have proved $(**)$. If condition (2) of $(*)$ does not hold, then

$$p^{i-1} \mathrm{Res}_{L_i/K} \mathrm{Cor}_{L_i/K} [(L/L_i, \tau_i, b)] = 0 \quad \text{for some } b \in T_i.$$

As we have seen, this implies that $\mathrm{Res}_{L_1/K} \mathrm{Cor}_{L_1/K} [(L/L_1, \tau_1, b)] = 0$. But $\bar{b} \in \bar{T}_i$ so since condition (2) of $(*)$ holds for $\bar{T}_i$,

$$p^{i-1} \mathrm{Res}_{\bar{L}_i/\bar{K}} \mathrm{Cor}_{\bar{L}_i/\bar{K}} [(\bar{L}/\bar{L}_i, \bar{\tau}_i, \bar{b})] = \mathrm{Res}_{\bar{L}_1/\bar{K}} \mathrm{Cor}_{\bar{L}_1/\bar{K}} [(\bar{L}/\bar{L}_1, \bar{\tau}_1, \bar{b})] \neq 0.$$

By $(**)$ we conclude that $\mathrm{Res}_{L_1/K} \mathrm{Cor}_{L_1/K} [(L/L_1, \tau_1, b)] \neq 0$. This proves that condition (2) of $(*)$ is satisfied for T_i. Finally, suppose that condition (3) of $(*)$ does not hold for the T_i, $i=1, \ldots, n$. Then there will exist $b_1, \ldots, b_r \in \bigcup_{i=1}^{n} T_i$ and $a_1, \ldots, a_r$ integers with $p \nmid a_j$ for $j=1, \ldots, r$, such that $\mathrm{Res}_{L_1/K} \mathrm{Cor}_{L_1/K} [(L/L_1, \tau_1, b_1^{a_1} \cdots b_1^{a_r})] = 0$. But this is impossible by $(**)$ and the fact that each $\bar{b}_i$ lies in $\bigcup_{i=1}^{n} \bar{T}_i$. Thus we need only prove that $(**)$ holds.

Suppose that d is an element of the valuation ring of L_1 with $\bar{d} \neq 0$ and with $\mathrm{Res}_{\bar{L}_1/\bar{K}} \mathrm{Cor}_{\bar{L}_1/\bar{K}}[(\bar{L}/\bar{L}_1, \bar{\tau}_1, \bar{d})] \neq 0$. We must show that $\mathrm{Res}_{L_1/K} \mathrm{Cor}_{L_1/K}[(L/L_1, \tau_1, d)] \neq 0$. For $\theta \in \mathrm{Gal}(L/K)$, let c_θ denote the conjugation isomorphism between $B(L/L_1)$ and $B(L/\theta(L_1))$ [4], page 255. Since $\langle \tau_1 \rangle$ is cyclic of order p, $\langle \tau_1 \rangle \cap \langle \theta \tau_1 \theta^{-1} \rangle = \{1\}$ or $\langle \tau_1 \rangle$. It follows by [4], Proposition 9. 1, page 257, that

$$\mathrm{Res}_{L_1/K} \mathrm{Cor}_{L_1/K}[(L/L_1, \tau_1, d)] = \sum c_\theta[(L/L_1, \tau_1, d)]$$

where the sum is taken over certain $\theta \in \mathrm{Gal}(L/K)$ with $\theta(L_1) = L_1$. For such θ an easy computation shows that $c_\theta[(L/L_1, \tau_1, d)] = [(L/L_1, \theta\tau_1\theta^{-1}, \theta(d))]$. Let $\theta\tau_1\theta^{-1} = \tau_1^t$ and let $nt \equiv 1 \pmod{p}$. Then $[(L/L_1, \theta\tau_1\theta^{-1}, \theta(d))] = [(L/L_1, \tau_1^t, \theta(d)^{nt})] = [(L/L_1, \tau_1, \theta(d)^n)]$ by [9], Satz 3, page 66. Thus there are elements $\theta_1, \ldots, \theta_r$ of $\mathrm{Gal}(L/K)$ and integers $n_1, \ldots, n_r$ such that

$$\mathrm{Res}_{L_1/K} \mathrm{Cor}_{L_1/K}[(L/L_1, \tau_1, d)] = [(L/L_1, \tau_1, \theta_1(d)^{n_1}\theta_2(d)^{n_2} \cdots \theta_r(d)^{n_r})].$$

Set $e = \theta_1(d)^{n_1}\theta_2(d)^{n_2} \cdots \theta_r(d)^{n_r}$ and suppose $\mathrm{Res}_{L_1/K} \mathrm{Cor}_{L_1/K}[(L/L_1, \tau_1, d)] = 0$. Then $[(L/L_1, \tau_1, e)] = 0$ so $e = N_{L/L_1}(u)$ for some $u \in L$. Let $\hat{L}$, $\hat{L}_1$, and $\hat{K}$ denote, respectively, the completions of L, L_1, and K with respect to φ. Since $\mathrm{Gal}(\hat{L}/\hat{L}_1) \cong \mathrm{Gal}(L/L_1)$ we have $e = \prod_\rho \rho(u)$ where the product is taken over all $\rho \in \mathrm{Gal}(\hat{L}/\hat{L}_1)$. Since d is a unit in $\hat{L}_1$, so also is e. Since u and $\rho(u)$ have the same valuations in $\hat{L}$, $\rho(u)$ is also a unit in $\hat{L}$ for all $\rho \in \mathrm{Gal}(\hat{L}/\hat{L}_1)$. Reducing modulo the maximal ideal of the valuation ring of $\hat{L}$ yields $\bar{e} = \prod_\rho \rho(\bar{u})$ where the product is taken over all $\rho \in \mathrm{Gal}(\bar{L}/\bar{L}_1) \cong \mathrm{Gal}(L/L_1) \cong \mathrm{Gal}(\hat{L}/\hat{L}_1)$. It follows that $\bar{\theta}_1(\bar{d})^{n_1}\bar{\theta}_2(\bar{d})^{n_2} \cdots \bar{\theta}_r(\bar{d})^{n_r} = N_{\bar{L}/\bar{L}_1}(\bar{u})$. Thus, reversing the above argument, we conclude that $\mathrm{Res}_{\bar{L}_1/\bar{K}} \mathrm{Cor}_{\bar{L}_1/\bar{K}}[(\bar{L}/\bar{L}_1, \bar{\tau}_1, \bar{d})] = 0$. This contradicts our assumption and completes the proof of Theorem 8.

Corollary 9. *Let K be a finitely generated extension of a global field and let L be a separable extension of K of prime degree p. Then $B(L/K) \cong \bigoplus_\omega Z(p)$.*

Proof. Let E be a Galois closure of L over K. Since $\mathrm{Gal}(E/K)$ is a subgroup of the symmetric group on the p roots of $\mathrm{Irr}(\alpha, K)$ where $L = K(\alpha)$, $p^2 \nmid [E:K]$. By Theorem 8, $B(E/K)_p \cong \bigoplus_\omega Z(p)$. Since $p \nmid [E:L]$, every element of $B(E/K)$ of order p is split by L so $B(L/K) \cong \bigoplus_\omega Z(p)$.

We conclude by posing three natural questions raised by Theorem 8. Let K be a finitely generated extension of a global field, let L be a finite dimensional Galois extension of K and let p^n equal the exponent of a Sylow p-subgroup of $\mathrm{Gal}(L/K)$.

Question 1. Is $B(L/K)$ of relative Brauer type?

Question 2. Can $B(L/K)_p$ have a direct summand isomorphic to $\bigoplus_\omega Z(p^m)$ for some $m > n$?

Question 3. Suppose M is a finite extension of K. Must $B(M/K) \neq \{0\}$? Must $B(M/K)$ be infinite?

Note added in proof. The authors have recently extended the results of § 4 to prove that if L is a non-trivial finite algebraic extension of K with K finitely generated over a global field, then $B(L/K)$ is infinite; in particular, both questions posed in Question 3 have affirmative answers.

References

[1] *E. Artin*, Algebraic Numbers and Algebraic Functions, New York 1967.
[2] *E. Artin* and *J. Tate*, Class Field Theory New York 1968.
[3] *A. Borel* and *J. Tits*, Elements unipotents et sousgroupes paraboliques de groupes réductifs. I, Invent. Math. **12** (1971), 95—104.
[4] *H. Cartan* and *S. Eilenberg*, Homological Algebra, Princeton 1956.
[5] *R. W. Carter*, Simple groups of Lie type, London 1972.
[6] *J. W. S. Cassels* and *A. Fröhlich*, Algebraic Number Theory, Washington 1967.
[7] *B. N. Cooperstein*, Minimal degree for a permutation representation of a classical group, Israel J. Math. **30** (1978), 213—235.
[8] *B. N. Cooperstein*, Subgroups of exceptional groups of Lie type generated by long root elements. I, II, to appear.
[9] *M. Deuring*, Algebren, Berlin-Heidelberg-New York 1968.
[10] *B. Fein* and *M. Schacher*, Relative Brauer groups. I, J. reine angew. Math. **321** (1981), 179—194.
[11] *A. Fröhlich*, On non-ramified extensions with prescribed Galois group, Mathematica **9** (1962), 133—134.
[12] *D. Gorenstein*, The classification of the finite simple groups. I, Simple groups and local analysis, Bull. AMS **1** (1979), 43—199.
[13] *G. H. Hardy* and *E. M. Wright*, Introduction to the theory of Numbers, London 1954.
[14] *B. Huppert*, Endliche Gruppen. I, Berlin-Heidelberg-New York, 1967.
[15] *N. Jacobson*, Lectures in Abstract Algebra. III, Princeton 1964.
[16] *W. M. Kantor*, Subgroups of classical groups generated by long root elements, Trans. AMS **248** (1979), 347—379.
[17] *H. Koch*, Galoissche Theorie der p-Erweiterungen, Berlin-Heidelberg-New York 1970.
[18] *S. Lang*, Diophantine Geometry, New York 1962.
[19] *J. Neukirch*, Klassenkörpertheorie, Mannheim 1969.
[20] *I. Reiner*, Maximal Orders, New York 1975.
[21] *P. Roquette*, Analytic theory of elliptic functions over local fields, Göttingen 1970.
[22] *M. Schacher*, Subfields of division rings. I, J. Algebra **9** (1968), 451—477.
[23] *M. Schacher*, Subfields of division rings. II, J. Algebra **10** (1968), 240—245.
[24] *A. Scholz*, Totale Normenreste, die keine Normen sind, als Erzeuger nicht abelscher Körpererweiterungen. II, J. reine angew. Math. **182** (1940), 217—234.
[25] *G. Seitz*, Flag-transitive subgroups of Chevalley groups, Annals of Math. **97** (1973), 27—56.
[26] *M. Suzuki*, On a class of doubly transitive groups, Annals of Math. **75** (1962), 105—145.
[27] *P. L. Tchebychef*, Memoire sur les nombres premiers, Mém. Ac. Sc. St. Petersbourg **7** (1850), 17—33.
[28] *A. Weil*, Basic Number Theory, Berlin-Heidelberg-New York 1974.
[29] *E. Weiss*, Algebraic Number Theory, New York 1963.
[30] *K. Zsigmondy*, Zur Theorie der Potenzreste, Monatsch. f. Math. u. Phys. **3** (1892), 265—284.

Department of Mathematics, Oregon State University, Corvallis, Oregon 97330, USA

Department of Mathematics, University of Oregon, Eugene, Oregon 97403, USA

Department of Mathematics, University of California, Los Angeles, California 90024, USA

Eingegangen 7. Januar 1981