Graded Brauer Groups

By *C. T. C. Wall* at Cambridge

This paper arose out of the observation that the definition of a Clifford algebra as an invariant of a quadratic form is made awkward by the fact that the algebra corresponding to the orthogonal direct sum of two quadratic forms is not simply the tensor product of their separate Clifford algebras. In fact, as is well known, the Clifford algebra admits a grading modulo 2, and we must consider the graded tensor product.

The object of this paper is to perform the theory of the Brauer group for graded algebras. We first define the class of central simple graded algebras over a field k, and then proceed to investigate their structure: we obtain a complete description. We then show that the class is closed under graded tensor products, and that the algebras, taken with a suitable equivalence relation, define a group, which we christen the graded Brauer group of k. The structure of this group is determined in terms of that of the ordinary Brauer group of k; in particular, if k is the real field, our group is cyclic of order 8. We then observe that taking the Clifford algebra of a quadratic form over k defines a homomorphism of the Witt group of k to the graded Brauer group; this image tells us essentially the determinant of the form, and an ungraded central simple algebra (one of the two Clifford algebras). A last paragraph clears up the case when k has characteristic 2, when a number of results are somewhat different; we obtain an equally complete theory, and, for example, the invariants of a quadratic form now reduce to the (ungraded) Clifford algebra and the Arf invariant.

Preliminaries

We first recall a number of standard results about ordinary (ungraded) central simple algebras over a field k. A convenient reference for these is [3].

(A) If A is a simple algebra (with unit) of finite dimension over a field k, then:

(i) A is isomorphic to a matrix algebra over a division ring, which contains k in its centre.

(ii) The centre of A is a field. (If this is k, A is *central* over k).

(iii) A has only one irreducible representation, and all representations are isomorphic to direct sums of it.

(B) Suppose A central simple, and B simple over k. Then:

(i) Any two imbeddings of B in A are conjugate in A. In particular,

(ii) Any automorphism of A is inner.

(iii) The algebra $A \otimes_k B$ is simple, with the 'same' centre as B.

(iv) If B is the opposite algebra, $\bar{A}$, to A, then $A \otimes_k \bar{A}$ is isomorphic to a matrix ring over k.

(v) If B is a simple subalgebra of A, C its centraliser, then C is simple. The centraliser of C is B. If B is central then $A \cong B \otimes_k C$.

Two central simple algebras are called equivalent if they are matrix rings over isomorphic division rings. It follows from standard properties of tensor products, with (Ai), (Biii) and (Biv), that the tensor product induces a multiplication of equivalence classes under which they form a group, which is called the Brauer group of k.

We shall also refer to quaternion algebras. If the characteristic of k is not 2, write k^* for the multiplicative group of nonzero elements of k. The algebra (a, b) admits a basis 1, U, V, UV, where $U^2 = a$, $V^2 = b$ and $VU = -UV$. This is always central simple; permuting U, V and UV we find $(b, a) \cong (a, b) \cong (a, -ab)$; also (a, b) depends only on the classes of a and b modulo squares in k^*. It is said to *split* if it is a matrix ring over k; this happens, for example, if $a = 1$. More generally we have, for the equivalence relation above,

$$(a, b) \otimes (a, c) \sim (a, bc).$$

If k has characteristic 2, use k for the additive group, and write $\wp x = x + x^2$. The algebra $(a, b]$, where $a \neq 0$, admits a basis 1, U, V, UV, where $U^2 = a$, $\wp V = b$, and $U^{-1} V U = V + 1$. This is central simple, and depends only on the classes of a and b in $k^*/(k^*)^2$ and $k/\wp(k)$. It splits if $a = 1$ or if $b = 0$, and we have

$$(a_1, b] \otimes (a_2, b] \sim (a_1 a_2, b]$$
$$(a, b_1] \otimes (a, b_2] \sim (a, b_1 + b_2].$$

If $b \neq 0$, we can interchange U and VU to show

$$(a, b] \cong (ab, b].$$

Elementary Properties

By 'algebra' we shall mean a finite dimensional associative algebra A with unit element 1 over the field k. We call A *graded* if it is expressed as the direct sum of two nonzero subspaces $A_0 \oplus A_1$ (where the suffices are integers modulo 2) and for each value of i, j, $A_i A_j \leqq A_{i+j}$. A subspace B of A is graded if it is the direct sum of the intersections $B \cap A_i$. For example, the centre $Z(A)$ is graded. For if $z_0 + z_1$ is central, and x belongs to A_0 or A_1, then by equating components in $xz_0 + xz_1 = z_0 x + z_1 x$ we see that x commutes with z_0 and z_1, which must then also be central.

We call the graded algebra A *central* if $Z(A) \cap A_0$ consists only of multiples of 1 (clearly it contains these), and *simple* if there are no proper graded ideals. These definitions seem to be the natural generalisations from those in the ungraded case. We shall suppose for the rest of this paragraph that A is a central simple graded algebra; for the first three lemmas we do not use the fact that A is central.

Lemma 1. $A_1^2 = A_0$. *If I is a proper ideal in A_0, $I + A_1 I A_1 = A_0$ and $A_1 I + I A_1 = A_1$.*

Proof. If $A_1^2 \neq A_0$, $A_1^2 + A_1$ is a proper graded ideal.

Similarly, if I is an ideal in A_0, $I + IA_1 + A_1I + A_1IA_1$ is closed under left and right multiplication by A_0 and A_1, hence is an ideal, and is clearly graded. Thus it is improper, and if $I \neq 0$ the result follows.

Lemma 2. *If J is a proper ideal in A, then the projections $\pi_i : J \to A_i$ $(i = 0, 1)$ are isomorphisms.*

Proof. $J \frown A_0$ and $\pi_0(J)$ are ideals in A_0. If these are equal, J is graded, which contradicts simplicity. If either is the ideal, I, of A_0, multiply on left and right by A_1 (using the fact that J is an ideal in A): we deduce $A_1IA_1 < I$, so by Lemma 1, I cannot be proper. Thus $J \frown A_0 = 0$, $\pi_0(J) = A_0$.

Hence $J \frown A_1 = A_0(J \frown A_1) = A_1^2(J \frown A_1) < A_1(J \frown A_0) = A_1 0 = 0$, and $\pi_1(J)$ contains $A_1\pi_0(J) = A_1$. Thus the π_i are both onto, and have zero kernels, as stated.

Lemma 3. *Either A is simple (as ungraded algebra) or A_0 is simple and $A_1 = A_0 u$, with $u \in Z(A) \frown A_1$ and $u^2 = 1$.*

Proof. Suppose A not simple: then it has a proper ideal J, and we can apply Lemma 2. Put $u = \pi_1\pi_0^{-1}(1)$. Then J contains $1 + u$ and so, being an ideal, also $u(1 + u) = u^2 + u$, $z(1 + u) = z + zu$ and $(1 + u)z = z + uz$. Since, by Lemma 2, an element of J is determined by either component, we have $u^2 = 1$, and for z in A_0 or A_1, $zu = uz$, so u is central. Then $A_1 = A_1 1 = A_1 u^2 < A_0 u$, and so $A_1 = A_0 u$.

Finally, if I is an ideal of A_0, we have

$$A_1 I A_1 = A_0 u I A_0 u = A_0 u I u = A_0 I u^2 = A_0 I = I,$$

and by Lemma 1, I is improper. Thus A_0 is simple.

Lemma 4. *Either A or A_0, but not both, is a central simple algebra over k (ungraded).*

Proof. If A is central, by Lemma 3 it is also simple. If not, the centre $Z(A)$ has a nonzero component V in A_1. Then $V^2 < Z(A) \frown A_0 = k$. If for some $v \neq 0$ in V, $v^2 = 0$, $Z(A)$ is not a field. Thus by (Aii) A is not simple, and by Lemma 3 we can find u with $u^2 = a \neq 0$ in k. So such a u exists in any case and now, as above, $A_1 = A_1 a = A_1 u^2 < A_0 u$, and so equals it. Since u is central, it follows that any $z \in Z(A_0)$ centralises all of A, so lies in k, thus A_0 is central. If I is an ideal of A_0, $I + Iu$ is a graded ideal of A, hence improper. So A_0 has no proper ideals and is simple.

Now suppose both A and A_0 central simple. Let B the centraliser of A_0 in A. By (Bv) B is central simple, and it is clearly a graded subspace (proof as for $Z(A)$) $B = B_0 \oplus B_1$ and $B_0 = k$. So B is also a graded central simple algebra. By Lemma 1, $B_1^2 \neq 0$; suppose then for $u, v \in B_1$ that $uv = 1$. Then $B_1 = B_1 1 = B_1 uv = B_0 v = kv$ is one-dimensional and B is commutative: a contradiction.

Structure Theory

We shall denote the case when A is central simple by (+) and when A_0 is so by (—).

Lemma 5. *In case (—), we have $A_1 = A_0 u$ with u central in A, $u^2 = a \neq 0$ in k. The centre of A coincides with the centraliser of A_0 and is $k + ku$, and the structure of A as graded algebra is completely determined by the structure of A_0 and the class of a modulo squares in k^*.*

Proof. The existence of u in A, central in A, with $u^2 = a \neq 0$ and hence $A_1 = A_0 u$ was established in the previous lemma. Any element of A centralising A_0

commutes also with u (since u is central) and so with $A_1 = A_0 u$ and is thus central in A. If $z \neq 0$ in A_1 is central in A, so is $zu \neq 0$ in A_0, hence this is some nonzero element, b say, of k. Then $za = zu^2 = bu$, so $z = bu/a$. Thus $Z(A) = k + ku$.

Clearly A_0 and a determine the structure of A — which is just the tensor product of A_0 and $Z(A)$. Conversely, A determines its zero-component A_0, and its centre $Z(A)$: the nonzero elements of $Z(A) \cap A_1$ are multiples cu ($c \in k^*$), and their squares $c^2 a$ determine a class modulo squares in k^*.

For the rest of this paper except the last paragraph, we shall now suppose that the characteristic of k is not 2; we shall see that analogous results do hold in that case, but it is somewhat inconvenient to consider the two cases together.

Lemma 6. *In case* $(+)$, *the centraliser of* A_0 *coincides with its centre, and is* $k + ku$, *where* $u^2 = a \neq 0$ *in* k. A_0 *is the centraliser of* u, *and* A_1 *the set of* y *in* A *with* $uy = -yu$. *The graded structure of* A *is completely determined by the ungraded structure and the choice (up to a scalar multiple) of* u *in* A *(not in* k*) with* $u^2 = a \neq 0$ *in* k.

Proof. Since we have excluded the characteristic 2 case, we consider the involution T of A defined by: $Tx = x$ for $x \in A_0$, and $Ty = -y$ for $y \in A_1$. This is clearly a nontrivial automorphism, and so, by (Bii), is inner; let u be the element of A, determined up to a scalar multiple, such that T is the inner automorphism by u. Since this leaves u fixed, $u \in A_0$; and by the definition of T, A_0 is the centraliser of u, and A_1 the set of y with $u^{-1} y u = -y$.

Now T is an involution, so u^2 induces the trivial automorphism of A, so is central. But u is regular, so $u^2 \neq 0$, and is thus a nonzero element a of k. A_0 is the centraliser of u, or equivalently, of $k + ku$. If a is not a perfect square in k, this is a field, hence by (Bv) equal to the centraliser of A_0; being contained in A_0, it is also the centre of A_0. (We shall give the proof for the case when a is a perfect square later). The last sentence of the lemma clearly follows from the preceding one (even if a is a square).

To obtain further insight into the structure of graded central simple algebras, we need to use the structure theorem (Ai) for ordinary central simple algebras. We first consider case $(+)$. The central simple algebra A is of the form $M_n(D)$, D a division ring. Let R be an irreducible A-module (e. g. a minimal right ideal). The centraliser of A in the ring of linear transformations of R is the anti-isomorph $\bar{D}$ of D. We have u in A_0, with $u^2 = a \neq 0$ in k, determining the structure. As $u \in A_0$, u commutes with $\bar{D}$, and A_0 is the centraliser of u (or of $k[u]$) in A, i. e. of $\bar{D} \otimes k[u]$ in the endomorphism ring of R. We have thus to study the ring $\bar{E} = \bar{D} \otimes k[u]$.

First suppose a not a square in k, and so $k[u]$ a field. Then since D is central simple over k, by (Biii), $\bar{E}$ is simple, with centre $k[u]$. Thus $\bar{E}$ is of the form $M_r(\bar{F})$, $\bar{F}$ a division algebra of centre $k[u]$. Now if $\bar{D}$ has degree d over k, $\bar{E}$ has degree $2d$, and an irreducible $\bar{E}$-module has dimension $2d/r$. But it is also a $\bar{D}$-module, so $2d/r$ is a multiple of d, and r is 1 or 2.

The case $r = 2$ occurs if and only if a vector space — say $\bar{D}$ — of dimension 1 over $\bar{D}$ admits an $\bar{E}$-module structure, i. e. if and only if $k[u]$ can be imbedded in the centraliser D of $\bar{D}$. If such an imbedding, ϑ, exists, it is (by (Bi)) unique up to conjugates in D, and if F is its centraliser (in D) we have $\bar{E} \cong M_2(\bar{F})$. This, as remarked above, is simple, and by (Aiii) R is a direct sum of n minimal right ideals. Thus we can choose a $\bar{D}$-basis with respect to which u is represented by a scalar matrix with diagonal elements $\vartheta(u)$, and $A_0 \cong M_n(F)$. In this case, the graded structure of A is determined by (n, D, a), where n is a positive integer, D a division ring with centre k, a an element of k^*, determined up to multiplication by nonzero squares, such that the quadratic extension $k[u]$ of k (where $u^2 = a$) can be imbedded in D.

Next consider the case $r = 1$: here $\bar{E}$ is a division ring. Then R is a vector space, of dimension m, say, over $\bar{E}$, and $n = 2m$. Its centraliser A_0 is isomorphic to $M_m(E)$. If we choose an $\bar{E}$-basis for R, we see that in the isomorphism $A \simeq M_{2m}(D)$, u can be represented by the matrix with diagonal blocks $\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}$. The graded structure of A is determined by (n, D, a) where now n is even and D, a are as before, but $k[u]$ cannot be imbedded in D.

Finally we must consider the case when a is a square in k; by multiplying u by a suitable element of k we may suppose $a = 1$. Then $k[u] \cong k \oplus k$: in fact, $\frac{1}{2}(1 \pm u)$ are orthogonal idempotents, and each generates a summand. Hence $\bar{E} \simeq \bar{D} \oplus \bar{D}$ is no longer simple, but remains semi-simple. For suitable p, q, R is isomorphic to the $\bar{E}$-module which is the direct sum of p copies of the first summand $\bar{D}$ and q of the second. We can take a matrix representation $A \cong M_{p+q}(D)$ in which u corresponds to the scalar matrix with p $(+1)$'s and then q (-1)'s down the diagonal. Hence $A_0 \cong M_p(D) \times M_q(D)$ and the unsettled case of Lemma 6 now follows, by an explicit calculation. The graded structure of A is determined by the unordered pair (p, q) of positive integers and the central division ring D.

In case $(-)$, we can write $A_0 \cong M_n(D)$ and describe the ungraded structure of A, with the same cases arising, depending whether $k[u]$ can be imbedded or not in D: in fact $A \cong M_{2n}(F)$, $M_n(E)$, $M_n(D) \oplus M_n(D)$ in the three cases, since, in general, $A \cong M_n(E)$.

We briefly summarise our results in

Theorem 1. *In case* $(-)$, *the structure of* A *is determined by the triple of invariants* (n, D, a), n *a positive integer*, D *a central division ring over* k, *and* a *a class in* k^* *modulo squares.*

In case $(+)$, *the same is in general true, provided* (i) *if the field* $k[u]$ (*where* $u^2 = a$) *cannot be imbedded in* D, *then* n *is even*, (ii) *if* $a = 1$, *we need also an unordered pair* (p, q) *of positive integers*, $p + q = n$.

Remark. The difficulty in case (ii) can be avoided, and some discussion shortened, if we impose an extra axiom that A_1 contains a regular element. We have avoided this, as it is unnecessary, and makes only this trivial difference to the class of algebras considered.

The Graded Brauer Group

Let A, B be two graded algebras over k, and C their graded tensor product. We remind the reader that as vector space, C is the same as the usual $A \otimes B$, but whereas $A \otimes 1$ usually commutes with $1 \otimes B$, we have, in the graded product,

$$(1 \otimes b_j)(a_i \otimes 1) = (-1)^{ij}(a_i \otimes 1)(1 \otimes b_j) \text{ for } a_i \in A_i,\ b_j \in B_j.$$

Theorem 2. *If A, B are graded central simple, then so is C.*

Proof. We first observe that the centraliser of $A_0 \otimes B_0$ is the graded tensor product of the centralisers (in A, B) of A_0 and B_0. For if $\{b_i\}$ is a base of B, the element $\Sigma\,(a_i \otimes b_i)$ of C centralises $A_0 \otimes 1$ if and only if the a_i centralise A_0: then if $\{\alpha_j\}$ is a base of the centraliser of A_0 in A, $\Sigma\,(\alpha_j \otimes \beta_j)$ centralises $1 \otimes B_0$ if and only if the β_j centralise B_0.

Now the centraliser of A_0 admits the base $(1, u)$ where $u \in A_1$ in case (—) (Lemma 5) and $u \in A_0$ in case (+) (Lemma 6), and $u^2 = a \neq 0$ in either case. Let v, b be the corresponding elements of B. Hence the centraliser of $A_0 \otimes B_0$ in C has base $(1, u, v, uv)$. But $C_0 = A_0 \otimes B_0 + A_1 \otimes B_1$; we next assert that the centraliser of C_0 has base $(1, uv)$. We leave verification that uv does centralise C_0 to the reader. Conversely, suppose (for $\alpha, \beta, \gamma, \delta \in k$) that $\alpha + \beta u + \gamma v + \delta uv$ centralises C_0.

If A and B have type (—), then u, v are in A_1, B_1 and $vu = -uv$, so

$$uv(\alpha + \beta u + \gamma v + \delta uv) = (\alpha - \beta u - \gamma v + \delta uv)\, uv.$$

Since uv is regular, the two terms in brackets are equal; as the characteristic is not 2, $\beta u + \gamma v = 0$.

If A has type (+), and B has type (—), then for any y in A_1,

$$yv(\alpha + \beta u + \gamma v + \delta uv) = (\alpha - \beta u - \gamma v + \delta uv)\, yv.$$

As the right hand side equals $(\alpha + \beta u + \gamma v + \delta uv)\, yv$, $2(\beta u + \gamma v)\, yv = 0$ whence, as v is regular, $(\beta u + \gamma v)\, y = 0$. This holds for all y in A_1, so $(\beta u + \gamma v)\, A_1 = 0$, and $\beta u + \gamma v \in (\beta u + \gamma v)\, A_0 = (\beta u + \gamma v)\, A_1^2 = 0$.

If A and B both have type (+), for $y \in A_1$ and $y' \in B_1$ we have

$$yy'(\alpha + \beta u + \gamma v + \delta uv) = (\alpha - \beta u - \gamma v + \delta uv)\, yy',$$

and so, as above, we deduce $(\beta u + \gamma v)\, A_1 B_1 = 0$ and thence $\beta u + \gamma v = 0$.

The centraliser of C_0 does, then, have base $\{1, uv\}$. Now if $uv \in C_0$, i. e. A and B have the same type, then uv is not central in C. For when the type of A and B is (+), we have $yuv = -uyv = -uvy$ for any y in $A_1 \otimes 1$; and when it is (—), $uuv = -uvu$. Thus in all cases, C is central.

Now suppose I a proper graded ideal in C. Then $I_0 = I \cap C_0$ is an ideal in C_0, and is proper (otherwise I would contain 1). Hence if $I_{00} = I_0 \cap (A_0 \otimes B_0)$ and I'_{00} is the projection of I_0 onto $A_0 \otimes B_0$, ignoring the component in $A_1 \otimes B_1$, I_{00} and I'_{00} are ideals in $A_0 \otimes B_0$.

But $A_0 \otimes B_0$, as (ungraded) tensor product of the algebras with known structure A_0 and B_0 is semi-simple; in fact a sum of 1, 2 or 4 isomorphic simple ideals. We can detect cases by looking at the centre of $A_0 \otimes B_0$ whose base consists of those of $(1, u, v, uv)$ which lie in $A_0 \otimes B_0$. For example, if $u \in A_0$ and $u^2 = 1$, and $v \in B_1$ or $v \in B_0$ with $v^2 \neq 1$, we have 2 simple ideals, with idempotents $\frac{1}{2}(1 \pm u)$. Since $uy = -yu$ for $y \in A_1$ in this case any ideal J with $A_1 J A_1 < J$ is improper. If u and v are both in the zero component, and an ideal J, with $A_1 J A_1 < J$, $B_1 J B_1 < J$, contains $\alpha + \beta u + \gamma v + \delta uv$ then it also contains

$$A_1(\alpha + \beta u + \gamma v + \delta uv)\, A_1 = (\alpha - \beta u + \gamma v - \delta uv)\, A_1^2,$$

and hence $\alpha + \gamma v$ and $\beta u + \delta u v$; similarly we see that it must contain α, βu, γv and $\delta u v$ separately, and so, unless all of these are zero, will contain 1.

Now the ideals I_{00} and I'_{00} defined above must, I being an ideal in C, have the properties $A_1 J A_1 < J$, $B_1 J B_1 < J$. By the preceding paragraph, they are improper. Since I_{00} does not contain 1, it is therefore zero. But I'_{00} is not zero (otherwise, I meets $A_1 \otimes B_1$ and hence — since $A_1^2 = A_0$, $B_1^2 = B_0$ — meets $A_0 \otimes B_0$ in a nonzero element, contradicting what we have just proved), so is the whole of $A_0 \otimes B_0$. We thus now have essentially the same situation as in Lemmas 2, 3 and so there is a w in $A_1 \otimes B_1$, central in C_0, with $w^2 = 1$, and I_0 the set of $z + zw$, $z \in A_0 \otimes B_0$. Since w is a nonzero element of the centraliser of $A_0 \otimes B_0$ we must have A and B of type (—), and $w = \lambda u v$ for some nonzero λ. But now I contains $1 + w$ and so also

$$u(1 + w)\, u = u(1 + \lambda u v)\, u = (1 - \lambda u v)\, u^2$$

and hence $1 - w$ so, finally 1 and I is improper, a contradiction.

We now wish to define a graded Brauer group; for this we must first collect our algebras in equivalence classes. In fact we define the *type* of a graded central simple algebra as the ordered triple (ε, a, D) of invariants, where $\varepsilon = \pm$ in the two cases of Lemma 4, D is the central division ring over k, and a the element of $k^*/(k^*)^2$ described in Theorem 1. We shall prove that the type of the graded tensor product of two graded central simple algebras depends only on their types, and that the types, under the multiplication so defined, form a group. We need first to reformulate our structure theory.

We write $\{a\}$ for the algebra of rank 2, with zero component generated by 1, and other component generated by u, with $u^2 = a1$.

Lemma 7. *If A has invariants $(-, n, a, D)$ then*

$$A \cong M_n(D) \otimes \{a\} \cong M_n(k) \otimes D \otimes \{a\}.$$

If A has invariants $(+, 2m, a, D)$ and (if $a = 1$) we have $p = q$, then

$$A \cong M_m(D) \otimes \{1\} \otimes \{-a\}.$$

Convention. An ungraded algebra may be regarded as graded, but with vanishing nonzero component; all tensor products are graded tensor products.

Proof. It follows directly from Lemma 5 that, in case (—), $A \cong A_0 \otimes \{a\}$, and (n, D) determine $A_0 \cong M_n(D)$.

In case (+) we represent u by the diagonal block matrix of $\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}$; this is certainly permissible when E is a division ring, and our argument showed that it is also permissible otherwise, if n is even and $a \neq 1$. In the case $a = 1$, observe that $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is equivalent to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, so taking u in this form is equivalent to assuming $p = q$. Now we take r with diagonal blocks $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$; since $ru = -ur$, then $r \in A_1$. Since $1, u, r$ and ur form a basis for the 2×2 matrices, which define a simple subalgebra, with centraliser $M_m(D)$, A is (by (Bv)) the tensor product of these subalgebras. Now take $s = ur$, then $sr = -rs$, $s^2 = -a$, and so r generates $\{1\}$, s generates $\{-a\}$, and the algebra of $1, u, r$ and s is the graded tensor product of these. The result follows.

Theorem 3. *The type of the graded tensor product of two graded central simple algebras depends only on those of the algebras. Multiplication of types is given by the formulae*

$$(1)\qquad (+, a, D) \otimes (+, a', D') = \big(+, aa', D \otimes D' \otimes (a, a')\big)$$

$$(2)\qquad (+, a, D) \otimes (-, a', D') = \big(-, aa', D \otimes D' \otimes (a, -a')\big)$$

$$(3)\qquad (-, a, D) \otimes (-, a', D') = \big(+, -aa', D \otimes D' \otimes (a, a')\big).$$

With the product, the types form a group.

Proof. We shall first establish formulae (1)—(3) in most cases, and then deduce the remaining cases, and the other clauses of the theorem. We have used the notation (a, a') for the quaternion algebra defined by a and a'; it may be defined as $\{a\} \otimes \{a'\}$ regarded as an ungraded algebra.

The proof of Theorem 2 shows that if u, u' are the canonically defined elements of the centralisers of the zero component in the two algebras, then $u \otimes u'$ fulfils the same role for their tensor product. The multiplication rules for the symbol $\pm$ and the invariant a follow at once. Rule (3) now follows from Lemma 7 and the calculation

$$\begin{aligned} D \otimes \{a\} \otimes D' \otimes \{a'\} &\cong D \otimes D' \otimes \{a\} \otimes \{a'\} \\ &\cong D \otimes D' \otimes (a, a') \end{aligned}$$

as ungraded algebra, since clearly the matrix ring does not change matters.

Next we consider $\{a_1\} \otimes \{a_2\} \otimes \{a_3\}$. Let u_1, u_2, u_3 be the basic elements in the 1-component of the three factors; then for the product, the centraliser of the 0-component is generated by $u_1 \otimes u_2 \otimes u_3$, with square $-a_1 a_2 a_3$, in the 1-component. Also, the 0-component of the product is the quaternion algebra whose basis consists of the elements $u_i \otimes u_j$ of square $-a_i a_j$. Hence we get

$$(4)\qquad \{a_1\} \otimes \{a_2\} \otimes \{a_3\} \cong \{-a_1 a_2 a_3\} \otimes (-a_1 a_2, -a_1 a_3).$$

Now if we assume that the algebras in case $(+)$ which appear are such that Lemma 7 applies, we can deduce (2) and (1) by:

$$D \otimes \{1\} \otimes \{-a\} \otimes D' \otimes \{a'\} \cong D \otimes D' \otimes \{aa'\} \otimes (a, -a')$$

and

$$D \otimes \{1\} \otimes \{-a\} \otimes D' \otimes \{1\} \otimes \{-a'\} \cong D \otimes D' \otimes \{1\} \otimes \{-aa'\} \otimes (a, a').$$

It follows that (2) and (1) are valid in general; we may remove the restriction that $n = 2m$ merely by noticing that taking tensor products with an ungraded $M_2(k)$ does not alter type, so that if this multiplication makes formulae (1) and (2) true, they must have been true already. To avoid the restriction $p = q$ we argue similarly that if $A_{p,q}$ stands for $M_{p+q}(k)$ graded with $A_0 \cong M_p(k) \oplus M_q(k)$, then $A_{1,1}$ acts as unit on types and $A_{p,q} \otimes A_{1,1} \cong A_{p+q,\, p+q}$. Now again, taking tensor products with $A_{1,1}$ of the two sides of an equation (1) or (2) makes it true, hence (as this operation does not affect type) it is true anyway.

This proves (1)—(3), and the first statement of the theorem. Now multiplication is clearly associative; we have just produced a unit $(+, 1, k)$, and we check explicitly (using (Biv)) that $\big(+, a, \bar{D} \otimes (a, a)\big)$ acts as inverse to $(+, a, D)$ and $(-, -a, \bar{D})$ to $(-, a, D)$ (recall that the algebra $(a, -a) \cong (a.\ 1)$ splits!), whence we have a group.

Thus, even in the separably closed case, the group so defined — which we call the graded Brauer group — has order 2. Next let k be arbitrary, and compute the powers of $x = (-, 1, k)$; we obtain, writing Q for $(-1, -1)$,

$$\begin{array}{ll} x^1 = (-, 1, k) & x^2 = (+, -1, k) \\ x^3 = (-, -1, Q) & x^4 = (+, 1, Q) \\ x^5 = (-, 1, Q) & x^6 = (+, -1, Q) \\ x^7 = (-, -1, k) & x^8 = (+, 1, k) = 1. \end{array}$$

Thus if $Q = (-1, -1)$ does not split (and so in particular, -1 is a non-square) we have a cyclic subgroup of order 8. In particular if k is the real field (or any real closed field), ± 1 are the only possibilities for a, and k and Q the only choices for D. So in this case the graded Brauer group is cyclic of order 8. This result (under various guises) has been known for a long time, and has emerged particularly clearly from work of R. Bott.

If we consider only algebras of case $(+)$, we obtain a subgroup of index 2 in the graded Brauer group, which we may call the little graded Brauer group. The product here is given by the simple formula (1). This admits a cohomological interpretation, similar to that of the ordinary Brauer group. In fact, write H^1 for $k^*/(k^*)^2$, the multiplicative group of k modulo squares, and H^2 for the usual Brauer group. Let us use additive notation for each of these. The quaternion algebras (a, a') give a symmetric bilinear pairing of H^1 with itself to H^2. Now if we write $1 + a + D$ to represent (formally) $(+, a, D)$ and interpret products aa' by the pairing above, aD, Da and DD' as zero, then formal multiplication yields the correct formula (1)

$$(1 + a + D)(1 + a' + D') = 1 + (a + a') + (D + aa' + D')$$

(recall that we replaced multiplicative by additive notation).

Let k_s be the separable closure of k, G the Galois group of k_s/k. Then the ordinary Brauer group is isomorphic to $H^2(G; k_s^*)$ and $k^*/(k^*)^2$ can be identified with $H^1(G; \mathbf{Z}_2)$. The cup product gives a pairing of this with itself to $H^2(G; \mathbf{Z}_2)$ and the mapping $\mathbf{Z}_2 \to k_s^*$ with image ± 1 induces an inclusion of $H^2(G; \mathbf{Z}_2)$ in $H^2(G; k_s^*)$; by a result of Delzant, the pairing of $H^1(G; \mathbf{Z}_2)$ into $H^2(G; k_s^*)$ coincides with the one used above. This gives the interpretation sought.

Application to Quadratic Forms

A quadratic form on a vector space V is (for us) a homogeneous quadratic mapping q of V to k whose induced bilinear map b $\big($where $b(x, y) = q(x + y) - q(x) - q(y)\big)$ induces an isomorphism of V with its dual. If the characteristic of k is not 2, then b determines q, for $b(x, x) = 2q(x)$. By a well known theorem, V admits an orthogonal basis $\{e_i\}$ for q.

The Clifford algebra $C(q)$ is the quotient of the tensor algebra of V by the ideal generated by relators $x \otimes x - q(x)$ $\big($note this contains $x \otimes y + y \otimes x - b(x, y)\big)$. Since these relators are homogeneous for the grading modulo 2, $C(q)$ inherits this grading from the symmetric algebra. Hence $C(q)$ is a graded algebra.

Theorem 4. *$C(q)$ is graded central simple. If (V, q) is the orthogonal direct sum of (V_1, q_1) and (V_2, q_2) then $C(q) \cong C(q_1) \otimes C(q_2)$.*

Proof. Since for $x_1 \in V_1$, $x_2 \in V_2$ we have $b(x_1, x_2) = 0$, in $C(q)$, $x_1 \otimes x_2 + x_2 \otimes x_1 = 0$. Now $C(q_1)$, $C(q_2)$ may clearly be regarded as subalgebras of $C(a)$; it follows from the remark above that the commutation rule between them is as usual. Hence we have a homomorphism of $C(q_1) \otimes C(q_2)$ to $C(q)$. This is onto since V generates $C(q)$ (as algebra); that it is $1-1$ follows since each relator for $C(q)$ has the form, for $x_i \in V_i$,

$$(x_1 + x_2) \otimes (x_1 + x_2) - q(x_1 + x_2) = (x_1 \otimes x_1 - q(x_1)) + (x_1 \otimes x_2 + x_2 \otimes x_1) + (x_2 \otimes x_2 - q(x_2)),$$

so is zero in $C(q_1) \otimes C(q_2)$.

This proves the second part of the theorem. The first part follows, on observing that (V, q) is an orthogonal direct sum of the subspaces (ke_i, q_i); that $C(q_i) = \{a_i\}$ if $q(e_i) = a_i$, so is graded central simple, and by applying Theorem 3.

Observe that $C(q)$ falls under case $(-)$ if the dimension, n, of V is odd; under case $(+)$ if n is even. This follows by induction. The invariant

$$a = (-1)^{\frac{1}{2}n(n-1)} \prod_i a_i = (-1)^{\frac{1}{2}n(n-1)} 2^{-n} \det b,$$

again by induction. These results are due to Witt [4].

It follows that the invariants of the graded algebra $C(q)$ tell us precisely the following: the dimension of V, the determinant of b, and the structure of a central simple algebra C or C_0. These are, of course, all standard invariants of q.

We can also verify by induction that the invariant D is of the form

$$\prod_{i<j} (a_i, a_j) \{\prod_i (-1, a_i)\}^{\frac{1}{2}(n-1)(n-2)} (-1, -1)^{\frac{1}{24}(n-1)(n-2)(n-3)(n-4)}.$$

Various methods have been used in the past to derive invariants satisfying simpler relations. Witt [4] takes as his invariants those of the Clifford algebra of $\sum_1^n a_i x_i^2 - \sum_{n+1}^{2n} x_j^2$.

This leads to an invariant

$$a = \prod a_i$$
$$D = \prod_{i<j} (a_i, a_j) \prod_i (-1, a_i) = \prod_{i \leq j} (a_i, a_j),$$

and the multiplication formula for a direct sum is given by formula (1) in all cases. This simplification has advantages; it also has the disadvantage that the class of $C(q)$ in the graded Brauer group (which certainly seems more natural) just vanishes for Witt kernels, and so defines a homomorphism of the Witt group. This is not case for the modified invariants above. Delzant (unpublished) has defined Stiefel classes, of which the first two run as follows: associate the quadratic form q_i with $(+, a_i, k)$ in the little graded Brauer group, and direct sums with products. This leads to $a = \prod_i a_i$ as above, and $D = \prod_{j<i} (a_i, a_j)$. This normalisation has the same disadvantages as discussed above; the compensating advantage in this case is that higher Stiefel classes are also obtained. Both these other normalisations give zero invariants to the form x^2 and generally to $\sum x_i^2$, rather than to Witt kernels.

Modifications in Characteristic 2

At a number of points above, we have used the hypothesis that the characteristic of k is not 2. We now verify that most of our results remain valid, after suitable changes, under the opposite assumption. The first and main difficulty is that the proof of Lemma 6 breaks down as T becomes trivial. We consider case $(+)$.

Lemma 8. (i) *A_0 is semi-simple.*

(ii) *A_0 is a sum of 1 or 2 simple ideals.*

Proof. (i) Let R be the radical of A_0. Then for some N, $R^N = 0$. Hence

$$(A_1 R A_1)^N < A_1 R^N A_1 = 0.$$

Thus $A_1 R A_1$ is a nilpotent ideal, hence contained in R. By Lemma 1, R is improper; since A_0 has unit, $R = 0$.

(ii) By (i), we can write $A_0 = \sum_{i=1}^{n} B_i$ as a sum of simple ideals. Now A_1 is a 2-sided A_0-module, hence a module over $\sum \bar{B}_i \otimes B_j$, so is a direct sum of modules C_{ij} over $\bar{B}_i \otimes B_j$. Now B_i is an ideal in A_0; by Lemma 1, $A_1 = A_1 B_i + B_i A_1$. But $B_i C_{jk} = 0$ for $i \neq j$, $B_i C_{ik} = C_{ik}$, and similarly for multiplying on the right. Hence

$$\sum_{j,k} C_{jk} = A_1 = A_1 B_i + B_i A_1 = \sum_j C_{ji} + \sum_k C_{ik},$$

so $C_{jk} = 0$ unless $k = i$ or $j = i$. Now if $n \geqq 3$, taking in turn $i = 1$, $i = 2$, $i = 3$ we deduce that each $C_{jk} = 0$, so $A_1 = 0$, a contradiction. Hence $n \leqq 2$ — and moreover, if $n = 2$, $A_1 = C_{12} + C_{21}$.

Lemma 9. *The centre of A_0 has degree 2 over k.*

Proof. We established in Lemma 8 that if A is central simple over k, and is graded, then A_0 is a sum of 1 or 2 simple ideals. Now if K is any (ungraded) extension of k, then $A \otimes K$ is central simple over K. We deduce that $A_0 \otimes K$ is still a sum of 1 or 2 simple ideals. Its centre, which is $Z(A_0) \otimes K$, is therefore a sum of 1 or 2 fields. We also observe that since, by Lemma 4, A_0 is not central simple, the degree of $Z(A_0)$ over k is not 1.

Now let A_0 be simple. $Z(A_0)$ is a field L of finite degree n over k. L is a separable extension of k, for otherwise let l be the separable closure of k in L. Then $L \otimes L$ is the centre of $A_0 \otimes L$, hence is a direct sum of fields, and so is the quotient algebra $L \otimes_l L$. But if $x \in L$ is inseparable over l, $x \otimes 1 + 1 \otimes x$ is nilpotent in $L \otimes_l L$: a contradiction. Hence L is separable, and if K is a normal extension of k containing L, L admits n distinct k-isomorphisms into K. These induce n distinct homomorphisms $L \otimes K \to K$, with comaximal kernels, and we deduce easily that $L \otimes K$ is the sum of n copies of K. But this is a sum of at most 2 fields, hence $n \leqq 2$ and so $n = 2$.

The argument when A_0 is a sum of two simple ideals runs the same way; taking L_1, L_2 as the centres of the two ideals, we must have $K \otimes L_1 + K \otimes L_2$ the sum of 2 fields for any K, and deduce that each L_i has degree 1.

Lemma 10. *$Z(A_0)$ is generated by an element u, with $u^2 + u = a \in k$. A_0 is the set of x in A with $xu = ux$. A_1 is the set of y in A with $y(1 + u) = uy$.*

Proof. First suppose A_0 simple. Then $Z(A_0)$ is a separable extension of degree 2, hence generated by x satisfying $x^2 + px + q = 0$ $(p \neq 0)$. We can write $u = x/p$; since $Z(A_0)$ is a field, $u^2 + u \neq 0$. Since u is in the centre of A_0, $u^{-1} x u = x$ for x in A_0; in fact A_0 is the centraliser of u by (Bv) and has half the dimension of A over k. Now A_1 is a module over $\bar{A}_0 \otimes A_0$ which admits just two homomorphisms to the matrix ring $\bar{A}_0 \otimes_{k[u]} A_0$, corresponding to the two imbeddings of $k[u]$ in the centre of $\bar{A}_0$. By the dimension condition, A_1 is an irreducible module over one of these rings (it is too small for anything else), and the fact that A_1 does not centralise u determines which. Hence $u^{-1} y (1 + u) = y$ for $y \in A_1$, and the characterisation of A_1 follows.

If A_0 is not simple, take u as the unit element in the first summand; then if v is the unit in the second, $u + v = 1$ and $uv = 0$. We have $A_0 = B_1 \oplus B_2$, $A_1 = C_{12} \oplus C_{21}$ and clearly u acts as left unit on B_1, C_{12}, left zero on B_2, C_{21}, right unit on B_1, C_{21}, and right zero on B_2, C_{12}; similarly for v. The characterisations of A_0 and A_1 follow.

Corollary. *The choice of u, with $u^2 + u \in k$, determines the grading of A.*

We now have an acceptable substitute for Lemma 6, and can complete the structure theory as before. Define $\wp(k)$ as the additive group of elements of k of the form $a^2 + a (a \in k)$; then a quadratic extension $k[u]$ determines $u^2 + u \in k$ up to adding an element of $\wp(k)$. The structure theory, without essential change, now gives

Theorem 1′. *In case* $(+)$, *in characteristic* 2, *the structure of A is determined in general by (n, D, a): n a positive integer, D a central division ring over k, a a class in k modulo $\wp(k)$. However* (i) *if the field $k[u]$ (where $u^2 + u = a$) cannot be imbedded in D, then n is even,* (ii) *if $a = 0$, so that $k[u] = ku \oplus k(1 + u)$, we need also an unordered pair (p, q) of positive integers, $p + q = n$.*

The formulation of the structure theory in Lemma 7 breaks down, however: although matrices $\begin{pmatrix} 0 & 1 \\ a & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ may now be taken for u and r, the algebra of u and r is indecomposable as a tensor product in case $(+)$. In fact Theorem 2 breaks down, for in characteristic 2 the graded tensor product coincides with the usual one, and its centre is the tensor product of theirs. So the tensor product of two algebras in case $(-)$ is not central. However, the tensor product of two algebras in case $(+)$ is another; this follows from (Biii). We now have

Theorem 3′. *In characteristic* 2, *multiplication of types is given by*

$$(+, a, D) \otimes (+, a', D') = (+, a + a', D \otimes D').$$

Proof. For the algebras themselves, we have simply

$$M_n(D) \otimes M_{n'}(D') = M_{nn'}(D \otimes D').$$

Now let u, u' be canonical elements in the centres of A_0, A_0'. Then the centre of $A_0 \otimes A_0'$ has basis $\{1, u, u', uu'\}$. We must find which of these centralise $A_1 \otimes A_1'$. Now by Lemma 10, for $y \in A_1$, $y' \in A_1'$,

$$yy'\{\alpha + \beta u + \gamma u' + \delta uu'\} = \{\alpha + \beta(u + 1) + \gamma(u' + 1) + \delta(u + 1)(u' + 1)\} yy',$$

and if for all y, y' this equals $\{\alpha + \beta u + \gamma u' + \delta uu'\} yy'$, then

$$\{\beta + \gamma + \delta(u + u' + 1)\} A_1 A_1' = 0,$$

whence $\beta + \gamma + \delta(u + u' + 1) = 0$ and so $\beta = \gamma$, $\delta = 0$. Hence $\{1, u + u'\}$ is a base of the centre of $(A \otimes A')_0$, and since $\wp(u + u') = \wp(u) + \wp(u')$, the result follows.

Thus in characteristic 2, only the little graded Brauer group can be defined, and this splits as a direct product.

We now turn to quadratic forms, and use the same notation as before. Since b is skew-symmetric and bilinear, we can choose a base $\{e_i, f_i\}$ of V such that b vanishes on all pairs of basis elements except $b(e_i, f_i) = 1$. The second part of Theorem 4 remains valid in our case, so we see that we need only study 2-dimensional V. If then, V has base $\{e, f\}$ with $q(e) = a$, $q(f) = a'$, $b(e, f) = 1$, then $C(q)$ has base $\{1, e, f, ef\}$ with $e^2 = a$, $f^2 = a'$, $ef + fe = 1$. We choose $v = ef$ — the usual element of the centraliser of A_0 — and $\wp v = efef + ef = effe = aa'$. Also $e^{-1}ve = fe = v + 1$. We have the central simple algebra $(a, aa']$.

Hence for any (nonsingular) quadratic form q, the algebra $C(q)$ is central simple, (this is the proof given by Arf [1]), and if $\{e_i, f_i\}$ is a canonical basis, our invariant a is $\sum_i q(e_i)\, q(f_i)$ $(\operatorname{mod} \wp(k))$, which is precisely the Arf invariant of q. This description of it is due to Kneser [2].

References

[1] *C. Arf*, Untersuchungen über quadratische Formen in Körpern der Charakteristik 2, Crelles Journal **183** (1941), 148—167.

[2] *M. Kneser*, Bestimmung des Zentrums der Cliffordschen Algebren einer quadratischen Form über einem Körper der Charakteristik 2. Crelles Journal **193** (1954), 123—125.

[3] *J.-P. Serre*, Applications algébriques de la cohomologie des groupes. Theorie des algèbres simples, Seminaire H. Cartan, Paris, 1950/51, exposés 6—7.

[4] *E. Witt*, Theorie der quadratischen Formen in beliebigen Körpern, Crelles Journal **176** (1937), 31—44.

Eingegangen 5. Juni 1963