

II. Brauer Factor Sets and Noether Factor Sets

In this chapter we consider the main classical results of the structure theory of central division algebras and more generally of central simple algebras over arbitrary fields. These center on two closely related problems: the determination of the algebras and the structure of the Brauer group $\text{Br}(F)$ of a field F .

We shall begin our discussion with a general construction of a central simple algebra A of degree n from a commutative Frobenius subalgebra K with $[K : F] = n$ and another element v of A . We show that v can be chosen so that $A = KvK$. Specialization to the case in which K is a commutative separable subalgebra gives rise to Brauer factor sets with values in the multiplicative group E^* of a splitting field E of K . The Brauer factor sets define a certain cohomology group $H^2(K/F)$ which is isomorphic to a subgroup of $\text{Br}(F)$. If K is a separable extension field this subgroup is the subgroup $\text{Br}(K/F)$ of $\text{Br}(F)$ of classes of central simple algebras over F split by K . Specialization to the case in which $K = E$ is Galois over F gives Noether factor sets and the fundamental isomorphism of $\text{Br}(E/F)$ with the cohomology group $H^2(G, E^*)$ where G is the Galois group $\text{Gal } E/F$ and the action of G on E^* is the natural one.

We use crossed products to show that $\text{Br}(F)$ is a torsion group and to derive the relations between the index and exponent of central simple algebras. We give an example due to Brauer to show that these relations are exact. After this we derive results of Wedderburn, Albert and Brauer on central division algebras of degree ≤ 5 . We then return to the general theory to derive the results on “inflation” and “restriction” for crossed products. The former leads to an isomorphism of the full Brauer group $\text{Br}(F)$ with a cohomology group of the Galois group G of the separable algebraic closure of F and an isomorphism of the e -torsion part $\text{Br}_e(F)$ of $\text{Br}(F)$ with a cohomology group $H_c^2(G, \mu_e)$ where μ_e is the set of the e^{th} roots of 1 (assuming $\text{char } F \nmid e$).

2.1. Frobenius Algebras

Definition. A finite dimensional associative algebra A over F is called a *Frobenius algebra* if A contains a hyperplane H that contains no non-zero one sided ideal of A .

If ℓ is a linear function on A . ℓ defines a bilinear form $\ell(a, b) = \ell(ab)$ which is *associative* in the sense that $\ell(ac, b) = \ell(a, cb)$. Any associative bilinear form $\ell(a, b)$ on A is obtained in this way since if $\ell(a) = \ell(a, 1)$ then $\ell(a, b) = \ell(ab, 1) = \ell(ab)$.

Let A be Frobenius, τ a linear function whose zeros constitute the hyperplane H that contains no one-sided ideal $\neq 0$ of A . If $\tau(a, b)$ is the bilinear form of τ then the set of z such that $\tau(a, z) = 0$ ($\tau(z, a) = 0$) for all $a \in A$ is a left (right) ideal contained in H . It follows that A is Frobenius if and only if there exists an associative non-degenerate bilinear form on A . We note also that if A is Frobenius and $\tau(a, b)$ is as indicated then for a left ideal I , the subspace $I^{\perp R} = \{c \mid \tau(I, c) = 0\}$ is the right annihilator $\text{ann}_R I$ of I . Hence this is a right ideal and $[I^{\perp R} : F] = n - [I : F]$. Similarly, if I is a right ideal then $I^{\perp L} = \{c \mid \tau(c, I) = 0\}$ is the left annihilator of I and $[I^{\perp L} : F] = n - [I : F]$. It follows that the map $I \rightsquigarrow I^{\perp R}$ is a lattice anti-isomorphism of the lattice of left ideals of A onto the lattice of right ideals.

If A is Frobenius then A_E is Frobenius for any extension field E/F . If $A = A_1 \oplus \cdots \oplus A_s$ where the A_i are ideals then A is Frobenius if and only if every A_i is Frobenius. We also have

Proposition 2.1.2. *If A and B are Frobenius algebras then $A \otimes_F B$ is a Frobenius algebra.*

Proof. Let τ and σ be linear functions on A and B respectively such that the corresponding hyperplanes contain no non-zero one-sided ideals. Let $\varphi = \tau \otimes \sigma$ be the linear function on $A \otimes B$ such that $\varphi(a \otimes b) = \tau(a)\sigma(b)$ for $a \in A, b \in B$. Let $z = \sum a_i \otimes b_i, a_i \in A, b_i \in B$, satisfy $\varphi(zc) = 0$ for all $c \in A \otimes B$. We may assume the a_i are linearly independent. Then there exist $x_i \in A$ such that $\tau(a_i x_j) = \delta_{ij}$. Let $y \in B$ and put $c = x_i \otimes y$. Then the condition $\varphi(zc) = 0$ gives $\sigma(b_i, y) = 0$. Since this holds for all $y, b_i = 0$ for all i and hence $z = 0$. Similarly $\varphi(cz) = 0$ for all c implies $z = 0$. It follows that the bilinear form $\varphi(c, d) = \varphi(cd)$ on $A \otimes B$ is non-degenerate. Hence $A \otimes B$ is Frobenius. \square

We shall derive next a condition that a commutative algebra A be a Frobenius algebra. We can write $A = A_1 \oplus \cdots \oplus A_s$ where the A_i are ideals and are local algebras (BA II, p. 111). For such an algebra we have

Proposition 2.1.3. *A local commutative algebra is Frobenius if and only if it contains a unique minimal ideal.*

Proof. Let A be a local commutative Frobenius algebra. Since A contains a unique maximal ideal it follows from the anti-automorphism of the lattice of ideals of A that A contains a unique minimal ideal. Conversely, suppose A is a commutative algebra that contains a unique minimal ideal N . We can choose a hyperplane H not containing N . Then H contains no non-zero ideal of A and hence A is Frobenius. \square

Corollary 2.1.4. *Any algebra $A = F[a]$ with a single generator is Frobenius.*

Proof. Let $f(\lambda)$ be the minimum polynomial of a and let $f(\lambda) = \prod_1^s p_i(\lambda)^{e_i}$ where the $p_i(\lambda)$ are distinct primes in $F[\lambda]$. Then $A = F[a_1] \oplus \cdots \oplus F[a_s]$ where the minimum polynomial of a_i is $p_i(\lambda)^{e_i}$. Now every ideal $\neq 0$ in $F[a_i]$ contains the ideal generated by $b_i = p_i(\lambda)^{e_i-1}$. Hence $F[a_i]$ contains a unique minimal ideal and so this is a Frobenius algebra. Then $F[a]$ is Frobenius. \square

The following module result will play a key role in obtaining a special type of generation of a central simple algebra by a commutative Frobenius subalgebra.

Proposition 2.1.5. *Let A be a commutative Frobenius algebra and let M be a faithful A -module. Then M contains a submodule isomorphic to A .*

Proof. Write $A = A_1 \oplus \cdots \oplus A_s$ where the A_i are local (BA II, pp. 425-427). Then A_i contains a unique minimal ideal N_i . We have $M = AM = A_1M \oplus \cdots \oplus A_sM$ and A_iM is a faithful A_i -module. Hence there exists an $x_i \in A_iM$ such that $N_i x_i \neq 0$. The map $a_i \rightsquigarrow a_i x_i$ is an A_i -homomorphism of A_i onto $A_i x_i$ which is a submodule of A_iM . The kernel of this homomorphism does not contain N_i . Since N_i is contained in every non-zero ideal of A_i the kernel is 0. Hence $A_i x_i \simeq A_i$ and $A_1 x_1 \oplus \cdots \oplus A_s x_s$ is a submodule of M isomorphic to A . \square

2.2. Commutative Frobenius Subalgebras

Let A be central simple. We can regard A as $A^e = A \otimes A^0$ module where A^0 is the opposite algebra of A by defining

$$(\Sigma a_i \otimes b_i)x = \Sigma a_i x b_i \quad (2.2.1)$$

where $a_i, x \in A, b_i \in A^0$ ($= A$ as vector space). Now A^e is simple since A and A^0 are central simple. Hence A is a faithful A^e -module (that is, the corresponding representation is faithful). If K is a subalgebra of A then restricting the action of A^e to $K^e = K \otimes K^0$ makes A a K^e -module and, of course, this is faithful. We now let K be a commutative Frobenius subalgebra whose dimensionality is the degree of A . Then we have

Theorem 2.2.2. *Let A be a central simple algebra of degree n , K a commutative Frobenius subalgebra of A such that $[K : F] = n$. Then A as $K^e = K \otimes K$ -module ($K^0 \simeq K$) is isomorphic to K^e and hence there exists a $v \in A$ such that $A = KvK$.*

Proof. The algebra K^e is a commutative Frobenius algebra and A is a faithful K^e -module. Hence, by 2.1.5, A contains a submodule isomorphic to K^e . On the other hand, $[A : F] = n^2 = [K^e : F]$. Hence $A \simeq K^e$ as K^e -module. Since K^e is cyclic with $1 \otimes 1$ as generator, A is cyclic as K^e -module. If v is a generator of this module then $A = K^e v = KvK$. \square

We shall require also

Theorem 2.2.3 (Jacobson [75]). *Let A and K be as in 2.2.2. Then: (1) $K = A^K$, the centralizer of K in A , (2) any isomorphism of K into A can be extended to an inner automorphism of A , (3) any derivation of K into A can be extended to an inner derivation of A .*

Proof. (1) Let $L = \text{End}_F K$. Then we have the isomorphism $k \rightsquigarrow k_L$ ($x \rightsquigarrow kx$) of K into L and we can identify K with its image K_L in L . Since K is commutative and the centralizer of the set of left multiplications of an algebra is the set of right multiplications, $L^K = K$. On the other hand, A^K can be characterized by the module condition $A^K = \{c \in A \mid (1 \otimes k - k \otimes 1)c = 0, k \in K\}$ and since A and L are K^e -isomorphic by 2.2.2 and $L^K = K$, we have $A^K = K$.

(2) We suppose first that $A = \text{End}_F V$ where V is an n dimensional vector space over F . Let σ be an isomorphism of K into A . We may regard V as K -module in two ways. In the first the action is the natural action of K as subalgebra of A and in the second it is the composite of the isomorphism σ with the natural action. Since V is faithful as K -module under both actions and $[V : F] = n$, it follows from 2.1.5 that the two K -modules we have defined on V are isomorphic. This means that there exists a bijective linear transformation u of V such that for every $k \in K$, $\sigma(k) = uku^{-1}$. Then $u \in A$ and σ can be extended to the inner automorphism I_u in $A = \text{End}_F V$.

Next let A be arbitrary. If A is split the result is covered by the case $A = \text{End}_F V$. Hence we may assume A is not split and so by Wedderburn's theorem on the commutativity of finite division rings the base field F is infinite. If \bar{F} is the algebraic closure of F then $A_{\bar{F}}$ is split and $K_{\bar{F}}$ is a commutative Frobenius subalgebra of $A_{\bar{F}}$. Applying the result in this case we obtain an invertible element $\tilde{u} \in A_{\bar{F}}$ such that $\sigma(k)\tilde{u} = \tilde{u}k, k \in K$. Now let (e_1, \dots, e_{n^2}) be a base for A/F and hence for $A_{\bar{F}}/\bar{F}$ and let (k_1, \dots, k_n) be a base for K/F . Then we have $\tilde{u} = \sum_1^{n^2} \omega_\ell e_\ell$, $\omega_\ell \in \bar{F}$, and the conditions that $\sigma(k_i)\tilde{u} = \tilde{u}k_i$ are equivalent to a set Γ of homogeneous linear equations on the ω_ℓ with coefficients in F . It follows that if U denotes the F -space of A of elements u such that $\sigma(k_i)u = uk_i, 1 \leq i \leq n$, and \tilde{U} the \bar{F} subspace of $A_{\bar{F}}$ of elements \tilde{u} such that $\sigma(k_i)\tilde{u} = \tilde{u}k_i$, then $\tilde{U} = \bar{F}U \simeq U_{\bar{F}}$. The subset of invertible elements of

U is the open subset defined by $n(u) \neq 0$. Since the corresponding subset of \tilde{U} is not vacuous it follows that we have invertible u in A such that $\sigma(k_i)u = uk_i$ and hence such that $\sigma(k)u = uk$ or $\sigma(k) = uku^{-1}, k \in K$. Thus σ can be extended to the inner automorphism I_u of A .

(3). Let δ be a derivation of K into A . Then $\delta \in L = \text{End}_F K$ and the condition $\delta(k\ell) = k(\delta\ell) + (\delta k)\ell$ for $k, \ell \in K$ is equivalent to the operator condition $\delta k_L = k_L\delta + 1(\delta k)_L$. Now suppose $\delta \rightsquigarrow d$ and $1 \rightsquigarrow v$ under a k^ℓ -isomorphism of L into A . Then we have $dk_L = k_Ld + v(\delta K)_L$ and $v \in k$ since $1k_L = K_L1$ implies that $v \in A^K = K$. Moreover, $1K_L = K_L$ gives vK which implies that v is invertible. Hence we have $(dv^{-1})k_L = k_L(dv^{-1}) + (\delta k)_L$ so δ can be extended to the inner derivation $x \rightsquigarrow (dv^{-1})x - x(dv^{-1})$ in A . \square

2.3. Brauer Factor Sets

Let A be central simple of degree n . We have shown in 1.6.20 that if the base field F is infinite then A contains an element u such that the minimum polynomial $f(\lambda)$ is of degree n with distinct roots. It is readily seen that the same result holds for finite A . For, in this case, $A \simeq M_n(F)$ and we can choose $f(\lambda)$ to be an irreducible polynomial of degree n over F . Then $M_n(F)$ contains a matrix whose minimum polynomial is $f(\lambda)$.

Now let $K = F[u]$ be a subalgebra of A such that the minimum polynomial $f(\lambda)$ over F of u is of degree n with distinct roots. Then K is a commutative Frobenius subalgebra of A and hence, by 2.2.2, A contains an element v such that $A = KvK$. Let E be a splitting field over F for $f(\lambda)$ so $E = F(r_1, r_2, \dots, r_n)$ where the r_i are distinct and $f(\lambda) = \prod(\lambda - r_i)$ in $E[\lambda]$. Consider the algebra $K_E = E[u] \simeq E[\lambda]/(f(\lambda))$. In this algebra we have n non-zero orthogonal idempotents

$$e_i = \frac{(u - r_1) \cdots (u - r_{i-1})(u - r_{i+1}) \cdots (u - r_n)}{(r_i - r_1) \cdots (r_i - r_{i-1})(r_i - r_{i+1}) \cdots (r_i - r_n)} \quad (2.3.1)$$

such that $\sum e_i = 1$ (see e.g. BA II, p. 479). Hence $K_E = \bigoplus_1^n Ee_i$. Now A_E is central simple of degree n over E and K_E contains the n orthogonal idempotents e_i . It follows that $A_E = M_n(E)$ so E is a splitting field for A . Thus we may regard A as an F -subalgebra of $M_n(E)$ such that $EA = M_n(E)$. Also we may suppose that

$$u = \text{diag}\{r_1, r_2, \dots, r_n\}. \quad (2.3.2)$$

If $v = (v_{ij})$ then $u^k v u^\ell = (r_i^k r_j^\ell v_{ij})$ and since $A = KvK$ the elements $u^k v u^\ell$, $0 \leq k, \ell \leq n-1$, form a base for A/F . Hence every element of A is a matrix

$$L = (\ell_{ij} v_{ij}) \quad (2.3.3)$$

where

$$\ell_{ij} = \sum_{k, \ell=1}^n a_{k\ell} r_i^{k-1} r_j^{\ell-1} \quad (2.3.4)$$

and the $a_{k\ell} \in F$ and are uniquely determined. Since $EA = M_n(E)$ it is clear that every $v_{ij} \neq 0$.

Let $G = \text{Gal } E/F$. If $\sigma \in G, \sigma r_i = r_{i'}$ and σ is determined by the permutation $i \rightsquigarrow i'$ of $\{1, 2, \dots, n\}$. We denote this permutation by σ also, so we have $\sigma r_i = r_{\sigma i}$. If ℓ_{ij} , $1 \leq i, j \leq n$, is defined by (2.3.4) then the ℓ_{ij} satisfy

$$\sigma \ell_{ij} = \ell_{\sigma i; \sigma j}, \quad \sigma \in G. \quad (2.3.5)$$

These conditions, which we shall call the *conjugacy conditions* on $\ell = (\ell_{ij})$, are also sufficient that the ℓ_{ij} have the form (2.3.4); for we have

Lemma 2.3.6. *Let $\ell = (\ell_{ij})$ be a matrix of elements $\ell_{ij} \in E$ satisfying the conjugacy conditions (2.3.5). Then there exist $a_{k\ell} \in F$ such that (2.3.4) holds for all i, j .*

Proof. Let V be the Vandermonde matrix

$$V = \begin{pmatrix} 1 & r_1 & r_1^2 & \cdots & r_1^{n-1} \\ 1 & r_2 & r_2^2 & \cdots & r_2^{n-1} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 1 & r_n & r_n^2 & \cdots & r_n^{n-1} \end{pmatrix}. \quad (2.3.7)$$

Then V is invertible. Hence there exists a unique matrix $a = (a_{ij}) \in M_n(E)$ such that

$$Va(tV) = \ell. \quad (2.3.8)$$

This matrix relation is equivalent to the equations (2.3.4). Applying $\sigma \in G$ to these equations we obtain

$$\ell_{\sigma i, \sigma j} = \sum_{k, \ell} (\sigma a_{k\ell}) r_{\sigma i}^{k-1} r_{\sigma j}^{\ell-1}$$

or $\ell_{ij} = \sum_{k, \ell} (\sigma a_{k\ell}) r_i^{k-1} r_j^{\ell-1}$. By the uniqueness of a we have $\sigma a_{k\ell} = a_{k\ell}$ for every $\sigma \in G$. Hence $a_{k\ell} \in F$. \square

(The foregoing proof is due to Walter Feit.)

We now put $L = (\ell_{ij} v_{ij}), L' = (\ell'_{ij} v_{ij})$ where the ℓ_{ij} and ℓ'_{ij} satisfy the conjugacy conditions, so $L, L' \in A$. Then $LL' = L'' = (\ell''_{ij} v_{ij})$ where

$$\ell''_{ij} = \sum_k \ell_{ik} c_{ikj} \ell'_{kj} \quad (2.3.9)$$

$$c_{ikj} = v_{ik} v_{kj} v_{ij}^{-1}. \quad (2.3.10)$$

Lemma 2.3.11. *The c_{ijk} satisfy*

$$\sigma c_{ijk} = c_{\sigma i, \sigma j, \sigma k} \quad (2.3.12)$$

$$c_{ijk} c_{ik\ell} = c_{ij\ell} c_{jk\ell} \quad (2.3.13)$$

Proof. Apply σ to (2.3.9) to obtain $\ell''_{\sigma i, \sigma j} = \sum_k \ell_{\sigma i, \sigma k} (\sigma c_{ikj}) \ell'_{\sigma k, \sigma j}$. On the other hand, $\ell''_{\sigma i, \sigma j} = \sum_k \ell_{\sigma i, \sigma k} c_{\sigma i, \sigma k, \sigma j} \ell'_{\sigma k, \sigma j}$. Hence we have

$$\sum_k \ell_{\sigma i, \sigma k} (\sigma c_{ikj} - c_{\sigma i, \sigma k, \sigma j}) \ell'_{\sigma k, \sigma j} = 0$$

or

$$\sum_k \ell_{ik} d_{ikj} \ell'_{kj} = 0, \quad d_{ikj} = \sigma c_{\sigma^{-1}i, \sigma^{-1}k, \sigma^{-1}j} - c_{ikj} \quad (2.3.14)$$

and these relations hold for all ℓ_{ik}, ℓ'_{jk} satisfying the conjugacy conditions. We can also write

$$\sum_k \ell_{ik} e_{ikj} (v_{kj} \ell'_{kj}) = 0, \quad e_{ikj} = d_{ikj} v_{kj}^{-1}. \quad (2.3.15)$$

Now $M_n(F) = EA$. Hence taking a suitable E -linear combination of the matrices in A we obtain a matrix whose j -th column is $(0, \dots, 0, 1, 0, \dots, 0)$ where the 1 is in any chosen position. Using this linear combination of the relations (2.3.15) we obtain $\ell_{ik} e_{ikj} = 0$ for all k . Then $e_{ikj} = 0$ and $d_{ikj} = 0$ which is (2.3.12). Now (2.3.13) follows by direct verification using the definition (2.3.10). \square

We now define a *Brauer factor set* c to be an indexed set of elements $c_{ijk} \in E^*$, $1 \leq i, j, k \leq n$, such that

$$\sigma c_{ijk} = c_{\sigma i, \sigma j, \sigma k}, \quad \sigma \in G \quad (i)$$

$$c_{ijk} c_{ikl} = c_{ijl} c_{jkl}. \quad (ii)$$

The foregoing lemma states that the c_{ijk} defined by (2.3.10) from the element $v = (v_{ij})$ constitute a Brauer factor set. We shall call (i) the conjugacy conditions on the c_{ijk} . We note that these imply that

$$c_{ijk} \in F(r_i, r_j, r_k) \quad (iii)$$

For, if $\sigma \in \text{Gal } E/F(r_i, r_j, r_k)$ then $\sigma i = i, \sigma j = j, \sigma k = k$ and hence, by (i), $\sigma c_{ijk} = c_{ijk}$. Since this holds for every $\sigma \in \text{Gal } E/F(r_i, r_j, r_k)$, $c_{ijk} \in F(r_i, r_j, r_k)$ by the Galois correspondence. If we put $i = j = k$ and $j = k = \ell$ successively in (ii) we obtain

$$c_{iij} = c_{iii} = c_{jii}. \quad (iv)$$

We note also that if we take $c_{ijk} = 1$ for all i, j, k then we obtain a Brauer factor set. This Brauer factor set will play a distinguished role in the sequel and will be denoted as 1.

We have seen that if we define $c_{ijk} = v_{ij} v_{jk} v_{ik}^{-1}$ then $c = \{c_{ijk}\}$ is a Brauer factor set. Here $v = (v_{ij})$ is any element of A such that $A = KvK$. We now observe that c is independent of the imbedding of A in $M_n(E)$ provided that $u = \text{diag}\{r_1, r_2, \dots, r_n\}$ in the imbedding. For, if we have a second imbedding with this property then it follows from the Skolem-Noether Theorem and the

fact that the only matrices that commute with u are diagonal matrices that in the second imbedding we have $v = (d_i v_{ij} d_j^{-1})$ where $d_i \in E^*$. Then

$$(d_i v_{ik} d_k^{-1})(d_k v_{kj} d_j^{-1})(d_i v_{ij} d_j^{-1})^{-1} = v_{ik} v_{kj} v_{ij}^{-1} = c_{ikj}.$$

We shall now normalize v so that the corresponding factor set c is *reduced* in the sense that every $c_{iii} = 1$. By (iv) this implies $c_{ijj} = 1 = c_{jii}$ for all i, j . We remark that if $f(\lambda)$ is irreducible or, equivalently, K is a field then c is reduced if $c_{111} = 1$. For, in this case the permutation group of the r_i determined by G is transitive. Then $c_{111} = 1$ implies $c_{iii} = 1$. We now note that, by (2.3.10), $c_{iii} = v_{ii}$ so $\sigma v_{ii} = v_{\sigma i, \sigma i}$, $\sigma \in G$. Hence if we put $\ell_{ii} = v_{ii}^{-2}$, and $\ell_{ij} = 0$ if $i \neq j$, then the conjugacy conditions hold for the ℓ_{ij} so

$$y = \text{diag}\{v_{11}^{-1}, v_{22}^{-1}, \dots, v_{nn}^{-1}\} \in A. \quad (2.3.16)$$

Since y commutes with u , $y \in F[u]$ and we can replace v by yv . This normalization permits us to assume $v_{ii} = 1$ and hence $c_{iii} = 1$, that is, c is reduced.

We can now prove

Theorem 2.3.17. *Let $K = F[u]$ be finite dimensional separable, $f(\lambda)$ the minimum polynomial of u over F and let $E = F(r_1, \dots, r_n)$ be the splitting field of $f(\lambda)$ over F where $f(\lambda) = \Pi(\lambda - r_i)$ in $E[\lambda]$. Suppose $c = \{c_{ijk}\}$ is a reduced Brauer factor set with values in E^* and let $B(K, c)$ denote the subset of $M_n(E)$ of matrices $\ell = (\ell_{ij})$ such that $\sigma \ell_{ij} = \ell_{\sigma i, \sigma j}$, $\sigma \in G = \text{Gal } E/F$. Then $B(K, c)$ is an F -subspace of $M_n(E)$, and if we define a c -product $\ell_c \ell'$ for $\ell = (\ell_{ij})$, $\ell' = (\ell'_{ij}) \in B(K, c)$ as $\ell'' = (\ell''_{ij})$ where*

$$\ell''_{ij} = \sum_k \ell_{ik} c_{ikj} \ell'_{kj} \quad (2.3.18)$$

then $B(K, c)$ becomes a central simple associative algebra of degree n over F containing a subalgebra isomorphic to K . Moreover, the map

$$\ell = (\ell_{ij}) \rightsquigarrow L = (c_{ij1} \ell_{ij}) \quad (2.3.19)$$

is an isomorphism of $B(K, c)$ with an F -subalgebra A of $M_n(E)$. Conversely, every central simple algebra of degree n containing K as subalgebra can be obtained by this construction.

Proof. It is clear that $B = B(K, c)$ is an F -subspace of $M_n(E)$ and if ℓ''_{ij} is defined by (2.3.18) then

$$\begin{aligned} \sigma \ell''_{ij} &= \sum_k (\sigma \ell_{ik}) (\sigma c_{ikj}) (\sigma \ell'_{kj}) \\ &= \sum_k \ell_{\sigma i, \sigma k} c_{\sigma i, \sigma k, \sigma j} \ell'_{\sigma k, \sigma j} \\ &= \sum_k \ell_{\sigma i, k} c_{\sigma i, k, \sigma j} \ell'_{k, \sigma j} \\ &= \ell''_{\sigma i, \sigma j}. \end{aligned}$$

Hence B is closed under the c -multiplication. Consider the map defined by (2.3.19). Evidently this is F -linear and injective. The (i, j) -entry of the matrix product $(c_{ij1}\ell_{ij})(c_{ij1}\ell'_{ij})$ is

$$\begin{aligned} \sum_k c_{ik1}c_{kj1}\ell_{ik}\ell'_{kj} &= \sum_k c_{ij1}c_{ikj}\ell_{ik}\ell'_{kj} \quad \text{by (ii)} \\ &= c_{ij1}\ell''_{ij}. \end{aligned}$$

Hence the map is a homomorphism for multiplication. The image $A = \{L\}$ of B is an F -subspace of $M_n(E)$ closed under multiplication. Observe next that since $c_{iii} = 1$, any diagonal matrix satisfying the conjugacy conditions is fixed under (2.3.19). Then $1 \in A$ and 1 is the unit of A and of B . Hence A is an F -subalgebra of $M_n(E)$.

We note next that $r = \text{diag}\{r_1, r_2, \dots, r_n\} \in A$ and $F[r]$ is a subalgebra of A isomorphic to K . Next let $\ell_{ij} = 1$ for all i, j and let s be the corresponding matrix $(c_{ij1}\ell_{ij}) = (c_{ij1})$. Note that every entry of s is $\neq 0$. Now every matrix unit $e_{ii} \in E[r]$, and since $e_{ii}se_{jj}$ is a non-zero multiple of e_{ij} it is clear that $EA = M_n(E)$. Since $M_n(E)$ is simple A contains no nilpotent ideals $\neq 0$ and A is not a direct sum of more than one non-zero ideal. Hence by the Wedderburn structure theory, A is simple. Any element of the center of A is in the center of $M_n(E)$ and so is a scalar matrix. Such an element has pre-image under (2.3.19) that is a diagonal matrix $\text{diag}\{\ell_1, \dots, \ell_n\}$. The conditions $\sigma\ell_i = \ell_{\sigma i}$ and $\text{diag}\{\ell_1, \dots, \ell_n\}$ is a scalar matrix imply that this element is in $F1$. Hence A is central simple. Then $M_n(E) \simeq E \otimes_F A$ (BA II, Theorem 4.7, p. 218) and consequently A has degree n . The isomorphism of $B(K, c)$ with A now implies that $B(K, c)$ is central simple of degree n and $B(K, c)$ contains a subalgebra isomorphic to K .

Conversely, assume A is central simple of degree n containing $K = F[u]$. We have seen that $A = KvK$ and we can identify A with the F -subalgebra of matrices $(v_{ij}\ell_{ij})$ where $v = (v_{ij})$ has all its entries $\neq 0$ and (ℓ_{ij}) satisfies the conjugacy conditions. Moreover, if we define $c_{ikj} = v_{ik}v_{kj}v_{ij}^{-1}$ then $c = \{c_{ijk}\}$ is a Brauer factor set. By normalizing v we may assume c is reduced. Now we have $(v_{ij}\ell_{ij})(v_{ij}\ell'_{ij}) = (v_{ij}\ell''_{ij})$ where ℓ''_{ij} is given by (2.3.18). Hence the map $(\ell_{ij}) \rightsquigarrow (v_{ij}\ell_{ij})$ is an isomorphism of (B, c) onto A . \square

We shall now determine the elements $w \in A$ such that $A = KwK$. We claim that these are just the elements $w = (\ell_{ij}v_{ij})$ such that every $\ell_{ij} \neq 0$. We have seen that $E[u] = D = \Sigma Ee_{ii}$. It is clear that $DwD = M_n(E)$ for a matrix $w = (w_{ij})$ if and only if every $w_{ij} \neq 0$. On the other hand, $D = EK$ and hence $DwD = EKwEK = EKwK$. Now if $w \in A$ then $KwK \subset A$ and hence $KwK = E \otimes_F KwK$. Hence $A = KwK$ for $w \in A$ if and only if $w = (\ell_{ij}v_{ij})$ with every $\ell_{ij} \neq 0$.

We have associated with an element $v \in A$ such that $A = KvK$ a factor set $c = \{c_{ijk}\}$ where $c_{ijk} = v_{ij}v_{ik}^{-1}$ for $v = (v_{ij})$. If $w = (\ell_{ij}v_{ij})$ where the ℓ_{ij} satisfy the conjugacy conditions and every $\ell_{ij} \neq 0$ then the Brauer factor set determined by w is $c' = \{c'_{ijk}\}$ where

$$c'_{ijk} = \ell_{ij}\ell_{jk}\ell_{ik}^{-1}c_{ijk}. \quad (2.3.20)$$

Two Brauer factor sets related in this way by ℓ_{ij} satisfying the conjugacy conditions are called *associates*. These constitute an equivalence class. We denote the equivalence class of the Brauer factor sets all of whose $c_{ijk} = 1$, by 1 and the relation of associateness by \sim .

Theorem 2.3.21 *The algebras $B(K, c)$ and $B(K, c')$ are isomorphic under a map which is the identity on $K = F[\text{diag}\{r_1, \dots, r_n\}]$ if and only if c and c' are associated (reduced) factor sets.*

Proof. (Seligman) If $c'_{ijk} = c_{ijk}m_{ij}m_{jk}m_{ik}^{-1}$ for all i, j, k , where $\sigma m_{ij} = m_{\sigma i, \sigma j}$, then $(\ell_{ij}) \rightsquigarrow (\ell_{ij}m_{ij}^{-1})$ is an isomorphism of $B(K, c)$ onto $B(K, c')$. Because c and c' are reduced, all $m_{ii} = 1$, so it is the identity on K .

Conversely, suppose $B(K, c)$ and $B(K, c')$ are isomorphic by a map extending the identity on K . Note that in the proof of Theorem 2.3.17, the isomorphism (2.3.19) could be replaced by $\varphi_s : (\ell_{ij}) \rightsquigarrow L = (c_{ijs}\ell_{ij})$, for each fixed index s , $1 \leq s \leq n$. We have a corresponding map of $B(K, c')$ into $M_n(E)$, also denoted φ_s . Thus, for each s , $\varphi_s(B(K, c))$ and $\varphi_s(B(K, c'))$ are isomorphic F -subalgebras A, A' of $M_n(E)$, with $E \otimes A = M_n(E) = E \otimes A'$. The isomorphism of A and A' resulting from the original isomorphism of $B(K, c)$ and $B(K, c')$ and the maps φ_s thus extends to a unique E -linear isomorphism $M_n(E) \rightarrow M_n(E)$ fixing $E \otimes K$, the diagonal matrices in $M_n(E)$.

Therefore there is an invertible diagonal E -matrix $d^{(s)} = \text{diag}\{\lambda_1^{(s)}, \dots, \lambda_n^{(s)}\}$ for each s , such that

$$d^{(s)-1}(\ell_{ij}c_{ijs})d^{(s)} = (\ell'_{ij}c'_{ijs})$$

for all $(\ell_{ij}) \in B(K, c)$, where (ℓ'_{ij}) is the image of (ℓ_{ij}) under the given isomorphism $B(K, c) \rightarrow B(K, c')$. In particular, when $\ell'_{ij} = 1$ for all i, j , the pre-image $(m_{ij}) \in B(K, c)$ satisfies

$$c'_{ijs} = \lambda_i^{(s)-1} m_{ij} c_{ijs} \lambda_j^{(s)} \text{ for all } i, j, s.$$

Setting $s = j$ gives $1 = \lambda_i^{(j)-1} m_{ij} \lambda_j^{(j)}$, or $m_{ij} = \lambda_i^{(j)} \lambda_j^{(j)-1}$. From the above,

$$\begin{aligned} c'_{ijs} &= c_{ijs} \lambda_i^{(j)} \lambda_j^{(j)-1} \lambda_j^{(s)} \lambda_i^{(s)-1} \\ &= c_{ijs} m_{ij} m_{js} m_{is}^{-1}, \end{aligned}$$

so c and c' are associated. □

2.4. Condition for Split Algebra. The Tensor Product Theorem.

We retain the notations of the last section. We prove first

Theorem 2.4.1. *$B(K, c) \sim 1$ in the Brauer group $\text{Br}(F)$ (that is, $B(K, c) \simeq M_n(F)$) if and only if $c \sim 1$.*

Proof. Suppose $c \sim 1$. Then we may assume every $c_{ijk} = 1$. Hence the subalgebra A of $M_n(E)$ isomorphic to $B(K, c)$ contains the matrix v all of whose entries are 1. This matrix has rank 1 and hence the left ideal $M_n(E)v$ of $M_n(E)$ is minimal and so is n dimensional over E . It follows that $[Av : F] = n$. Then A has a representation by $n \times n$ matrices over F determined by the module Av . It follows that $A \simeq M_n(F)$. Conversely, suppose $B(K, c) \simeq M_n(F)$. Then $B(K, c) \simeq B(K, 1)$. We have shown in 2.2.3 that if A is central simple of degree n and K_1 and K_2 are isomorphic commutative Frobenius subalgebras of A with $[K_i : F] = n$ then any isomorphism of K_1 onto K_2 can be extended to an inner automorphism of A . Hence if $B(K, c) \simeq B(K, 1)$ then we may assume that we have an isomorphism between these algebras that is the identity map on K . Let A_1 and A_2 be the subalgebras of $M_n(E)$ isomorphic to $B(K, 1)$ and $B(K, c)$ respectively by (2.3.19). Then A_i contains the matrix $u = \text{diag}\{r_1, r_2, \dots, r_n\}$, A_1 contains the matrix v_1 all of whose entries are 1 and A_2 contains $v_2 = (v_{ij})$ so that $c_{ijk} = v_{ik}v_{kj}v_{ij}^{-1}$. Then $A_1 = F[u]v_1F[u]$, $A_2 = F[u]v_2F[u]$ and we have an isomorphism η of A_2 onto A_1 that is the identity on u . Then $w_1 = \eta(v_2)$ satisfies $A_1 = F[u]w_1F[u]$ and we have seen that the Brauer factor set determined by w_1 is c . Since that determined by v_1 is 1 we have $c \sim 1$. \square

We consider next the tensor product of two central simple algebras A_i , $i = 1, 2$, of degree n containing $K = F[u]$ as subalgebra. Let v_i be an element of A_i such that $A_i = Kv_iK$ and let $v_i = (v_{jk}^{(i)})$ in an imbedding of A_i in $M_n(E)$. The algebra $A_1 \otimes_F A_2$ contains $K \otimes_F A_2$ which contains $K \otimes_F K$. We have the surjective algebra homomorphism

$$\nu : K \otimes_F K \rightarrow K \quad (2.4.2)$$

such that $\sum a_i \otimes b_i \rightsquigarrow \sum a_i b_i$. Since $K \otimes_F K$ is semi-simple (which is easily seen by extending F to its algebraic closure) we have

$$K \otimes_F K = (K \otimes_F K)e \oplus (K \otimes_F K)(1 - e) \quad (2.4.3)$$

where e is an idempotent and $(K \otimes_F K)(1 - e) = \ker \nu$. Then $(K \otimes K)e \simeq (K \otimes K)/\ker \nu \simeq K$. Moreover, since $a \otimes 1 - 1 \otimes a \in \ker \nu$ for $a \in K$, we have

$$(a \otimes 1)e = (1 \otimes a)e, \quad a \in K. \quad (2.4.4)$$

We now consider the algebra

$$A = e(A_1 \otimes_F A_2)e. \quad (2.4.5)$$

Since A_1 and A_2 are central simple so is $A_1 \otimes_F A_2$ and hence so is A . Moreover, A and $A_1 \otimes_F A_2$ determine the same element of the Brauer group $\text{Br}(F)$ and A contains $e(K \otimes_F K)e \simeq K$ which we can identify with K . Then we have

Theorem 2.4.6. *A is of degree n containing K , and a Brauer factor set associated with A as in (2.4.5) is $c^{(1)}c^{(2)} = \{c_{jkl}^{(1)}c_{jkl}^{(2)}\}$ where $c^{(i)} = \{c_{jkl}^{(i)}\}$ is a Brauer factor set associated with A_i .*

Proof. If $a^{(1)} = (\alpha_{ij}^{(1)})$, $a^{(2)} = (\alpha_{ij}^{(2)}) \in M_n(E)$ we define

$$a^{(1)} \otimes a^{(2)} = \begin{pmatrix} \alpha_{11}^{(1)}a^{(2)} & \alpha_{12}^{(1)}a^{(2)} & \cdots & \alpha_{1n}^{(1)}a^{(2)} \\ \alpha_{21}^{(1)}a^{(2)} & \alpha_{22}^{(1)}a^{(2)} & \cdots & \alpha_{2n}^{(1)}a^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1}^{(1)}a^{(2)} & \alpha_{n2}^{(1)}a^{(2)} & \cdots & \alpha_{nn}^{(1)}a^{(2)} \end{pmatrix} \quad (2.4.7)$$

and we use this tensor multiplication of matrices to obtain an imbedding of $A_1 \otimes_F A_2$ in $M_{n^2}(E)$. Since $u = \text{diag}\{r_1, r_2, \dots, r_n\}$ in $M_n(E)$ it is clear that the matrix for any $a \in K \otimes_F K$ in $M_{n^2}(E)$ is a diagonal matrix. Hence the matrix for e is diagonal with entries 0 and 1. Also we have

$$u \otimes 1 = \begin{pmatrix} r_1 1_n & & & \\ & r_2 1_n & & \\ & & \ddots & \\ & & & r_n 1_n \end{pmatrix} \quad (2.4.8)$$

$$1 \otimes u = \begin{pmatrix} u & & 0 \\ & \ddots & \\ 0 & & u \end{pmatrix} \quad (2.4.9)$$

Hence the condition (2.4.4) for $a = u$ implies that all the diagonal entries of e are 0 with the exception of those in the positions $1, n+2, 2n+3, \dots, n^2$. This implies that $eM_{n^2}(E)e$ has degree $\leq n$ and hence the degree of $e(A_1 \otimes A_2)e$ is $\leq n$. On the other hand, this degree is $\geq n$ since $A \supset K$. Hence A has degree n and the diagonal entries of e in the positions $1, n+2, \dots, n^2$ are 1 and the remaining ones are 0. The matrix $e(v_1 \otimes v_2)e$ in $M_{n^2}(E)$ has non-zero entries only in the $((k-1)n+k, (\ell-1)n+\ell)$, positions $1 \leq k, \ell \leq n$, and the entry in this position is $v_{k\ell}^{(1)}v_{k\ell}^{(2)}$.

By performing a similarity transformation by a permutation matrix and cutting down to a diagonal block we obtain an imbedding of A in $M_n(E)$ in which $u = \text{diag}\{r_1, \dots, r_n\}$ and $v = e(v_1 \otimes v_2)e = (v_{k\ell}^{(1)}v_{k\ell}^{(2)})$. Since all the entries of v are $\neq 0$, $M_n(E) = (\Sigma E e_{ii})v(\Sigma E e_{ii})$ and hence $A = KvK$. It follows that we can use v to determine a Brauer factor set for A . Evidently this set is $c^{(1)}c^{(2)}$. \square

2.5. The Brauer Group $\text{Br}(K/F)$

From now on we assume for simplicity that the base field F is infinite. As before, let K be a finite dimensional commutative separable algebra over F . If \bar{F} is the algebraic closure of F then $K_{\bar{F}} = \bar{F}e_1 \oplus \cdots \oplus \bar{F}e_n$ where the e_i are orthogonal idempotents and $n = [K : F]$. It follows that the degree of $K = \deg K_{\bar{F}} = n$. Hence, by Theorem 1.6.21, $K = F[u]$. Moreover, the minimum polynomial $f(\lambda)$ of u is of degree n and has distinct roots. We shall say that an extension field E/F *splits* K if $K_E = Ee_1 \oplus \cdots \oplus Ee_n$ where the e_i are orthogonal idempotents and we call E a *splitting field* for K if E splits K and no proper subfield of E splits K . It is readily seen that E is a splitting field for K/F if and only if E is a splitting field in the usual sense for the polynomial $f(\lambda)$. Hence any two splitting fields E/F and E'/F of K/F are isomorphic.

Now let E/F be a splitting field for K/F where $K = F[u]$ and $f(\lambda)$ is the minimum polynomial of u . Then E is a splitting field of $f(\lambda)$. For each root r of $f(\lambda)$ we have a homomorphism α of K/F into E/F such that $u \rightsquigarrow r$. In this way we obtain $n = [K : F]$ homomorphisms of K/F into E/F such that $\alpha_i u = r_i$ where $f(\lambda) = \prod (\lambda - r_i)$ in $E[\lambda]$. Moreover, this gives all the homomorphisms of K/F into E/F . Thus

$$M = \{\alpha_1, \alpha_2, \dots, \alpha_n\} \quad (2.5.1)$$

is the set of homomorphisms of K/F into E/F . If $\sigma \in G = \text{Gal } E/F$ then $\sigma\alpha_i \in M$. In fact, we have $\sigma\alpha_i u = \sigma r_i = r_{\sigma i}$ so $\sigma\alpha_i = \alpha_{\sigma i}$.

Now let $c = \{c_{ijk}\}$ be a Brauer factor set. We can regard this as a map c of $M \times M \times M$ into E^* such that

$$c : (\alpha_i, \alpha_j, \alpha_k) \rightsquigarrow c_{ijk}. \quad (2.5.2)$$

Accordingly, we write $c(\alpha_i, \alpha_j, \alpha_k)$ for c_{ijk} . Then the defining conditions on the c_{ijk} are first that

$$\sigma c(\alpha_i, \alpha_j, \alpha_k) = \sigma c_{ijk} = c_{\sigma i, \sigma j, \sigma k} = c(\sigma\alpha_i, \sigma\alpha_j, \sigma\alpha_k) \quad (2.5.3)$$

or, independently of the indexing,

$$\sigma c(\alpha, \beta, \gamma) = c(\sigma\alpha, \sigma\beta, \sigma\gamma), \quad \alpha, \beta, \gamma \in M. \quad (2.5.3')$$

We shall now call these conditions *homogeneity* and, more generally, if $g :$

$\overbrace{M \times \cdots \times M}^r \rightarrow E \text{ or } E^*$ then g is *homogeneous* if

$$g(\sigma\alpha, \sigma\beta, \dots, \sigma\varepsilon) = \sigma g(\alpha, \beta, \dots, \varepsilon) \quad (2.5.4)$$

for $\alpha, \beta, \dots, \varepsilon \in M$. In addition to this condition on c we have

$$c(\alpha, \beta, \gamma)c(\alpha, \gamma, \delta) = c(\alpha, \beta, \delta)c(\beta, \gamma, \delta) \quad (2.5.5)$$

for $\alpha, \beta, \gamma, \delta \in M$ and c is *reduced* if $c(\alpha, \alpha, \alpha) = 1$ for all $\alpha \in M$. This implies that $c(\beta, \alpha, \alpha) = 1 = c(\alpha, \alpha, \beta)$ for all α, β . If K is a field then c is reduced if $c(\alpha, \alpha, \alpha) = 1$ for a single $\alpha \in M$.

Similarly, a matrix $\ell = (\ell_{ij}) \in M_n(E)$ can be regarded as a map $(\alpha_i, \alpha_j) \rightsquigarrow \ell_{ij}$. The usual matrix product of ℓ and ℓ' can then be defined by $\ell\ell'(\alpha, \beta) = \sum_{\gamma \in M} \ell(\alpha, \gamma)\ell'(\gamma, \beta)$. Homogeneity of ℓ as map of $M \times M \rightarrow E$ is equivalent to the conjugacy conditions $\ell_{\sigma i, \sigma j} = \sigma \ell_{ij}$.

We can now re-state Theorem 2.3.17 in the following way:

Theorem 2.5.6. *Let K/F be a finite dimensional separable commutative algebra, E/F a splitting field for K/F , c a reduced Brauer factor set with values in E^* . Let $B(K, c)$ denote the F -space of homogeneous maps of $M \times M$ into E and define a product in $B(K, c)$ by*

$$\ell\ell'(\alpha, \beta) = \sum_{\gamma \in M} \ell(\alpha, \gamma)c(\alpha, \gamma, \beta)\ell'(\gamma, \beta) \quad (2.5.7)$$

for $\ell, \ell' \in B(K, c)$. Then $B(K, c)$ becomes a central simple algebra of degree $n = [K : F]$ containing a subalgebra isomorphic to K . Moreover, for any fixed $\gamma \in M$ the map $\ell \rightsquigarrow L$ where

$$L(\alpha, \beta) = c(\alpha, \beta, \gamma)\ell(\alpha, \beta) \quad (2.5.8)$$

is an isomorphism of $B(K, c)$ with an F -subalgebra A of the matrix algebra of maps of $M \times M$ into E . Conversely, any central simple algebra of degree n containing K as a subalgebra can be obtained in this way.

We shall call $B(K, c)$ the *Brauer algebra determined by the Brauer factor set c* . The condition that K is a commutative separable subalgebra of dimension equal to the degree is equivalent to two other conditions given in

Theorem 2.5.9. *Let A be central simple of degree n over F , K/F a commutative separable subalgebra of A . Then the following conditions on K are equivalent: (i) $[K : F] = n$, (ii) K is a maximal commutative separable subalgebra of A , (iii) the centralizer $A^K = K$.*

Proof. (i) \Rightarrow (ii). Suppose L is a commutative separable subalgebra of A containing K . Then $L = F[v]$ and the degree of the minimum polynomial of $v \leq \deg A = [K : F]$. Hence $[L : F] \leq [K : F]$ so $L = K$.

(ii) \Rightarrow (iii). Let K be a maximal commutative subalgebra of A . Then $K \subset A^K$. Now A^K is separable. For, if \bar{F} is the algebraic closure of F then $A_{\bar{F}} = M_n(\bar{F})$, $F_{\bar{F}} = \bar{F}e_1 \oplus \cdots \oplus \bar{F}e_m$ where the e_i are non-zero orthogonal idempotents such that $\sum e_i = 1$. Then $(A^K)_{\bar{F}} \simeq A_{\bar{F}}^{K_{\bar{F}}} = M_n(\bar{F})^{\sum \bar{F}e_i}$. It is clear that the last algebra is a direct sum of algebras $M_{n_i}(\bar{F})$. Hence A^K is separable. Then the center of A^K is separable and since it contains K it coincides with K by the maximality of K . Now $A^K = A_1 \oplus \cdots \oplus A_s$ where A_i is separable with separable center K_i and $K_1 + \cdots + K_s$. Suppose

for some $A_i \supsetneq K_i$. If A_i is not a division algebra then A_i contains $m \geq 2$ non-zero orthogonal idempotents f_j such that $\Sigma f_j = 1_i$ the unit of A_i . Then $K_1 + \cdots + K_{i-1} + \Sigma K_i f_j + K_{i+1} + \cdots + K_s$ is a commutative separable subalgebra of A properly containing K contrary to the maximality of K . The same conclusion holds if A_i is a division algebra since in this case A_i contains a separable subfield properly containing K_i . These contradictions show that $A_i = K_i$ for every i and hence $A^K = K$.

(iii) \Rightarrow (i) Suppose $A^K = K$. Then $A_{\bar{F}}^{K_{\bar{F}}} = K_{\bar{F}}$ for \bar{F} the algebraic closure of F and hence $M_n(\bar{F})^{\Sigma \bar{F} e_i} = \Sigma \bar{F} e_i$ where the e_i are non-zero orthogonal idempotents such that $\Sigma e_i = 1$ and $m = [K : F]$. It follows that $m = n$ and $[K : F] = n$. \square

The Brauer factor sets (regarded as maps of $M \times M \times M$ into E^*) form a group under multiplication of images in E^* . This contains the subgroup of factor sets such that

$$c(\alpha, \beta, \gamma) = \ell(\alpha, \beta) \ell(\beta, \gamma) \ell(\alpha, \gamma)^{-1} \quad (2.5.10)$$

where $\ell : M \times M \rightarrow E^*$ is homogeneous. We can form the factor group which we shall denote as $H^2(K/F)$. If c is a factor set then ℓ defined by $\ell(\alpha, \alpha) = c(\alpha, \alpha, \alpha)^{-1}$, $\ell(\alpha, \beta) = 1$ if $\alpha \neq \beta$ is homogeneous and $c(\alpha, \beta, \gamma) \ell(\alpha, \beta) \ell(\beta, \gamma) \ell(\alpha, \gamma)^{-1}$ is reduced. It follows that $H^2(K, F)$ is the factor group of the group of reduced Brauer factor sets with respect to its subgroup of reduced Brauer factor sets of the form (2.5.10).

We recall that an extension field K of the base field F of a central simple algebra A is called a splitting field for A if $A_K = K \otimes_F A \simeq M_n(K)$. If $[A]$ denotes the similarity class of A in the Brauer group $\text{Br}(F)$ then K is a splitting field for A if and only if it is a splitting field for every $B \in [A]$. Hence we may regard K as a splitting field of the class $[A]$. We have the homomorphism $[A] \rightsquigarrow [A_K]$ of $\text{Br}(F)$ into $\text{Br}(K)$ whose kernel is the subgroup $\text{Br}(K/F)$ of classes $[A]$ split by K , that is, having K as splitting field.

A classical theorem of Brauer and Noether gives a determination of the finite dimensional K that split a class $[A]$: Let Δ be a central division algebra over F . Then K splits Δ if and only if $[K : F] = rd$ where d is the degree of Δ and K is isomorphic to a subfield of $M_r(\Delta)$ (Theorem 4.12, p. 224 of BA II).

Now let K be finite dimensional separable over F . Then we have

Theorem 2.5.11. *$\text{Br}(K/F)$ is a subgroup of $\text{Br}(F)$ isomorphic to $H^2(K/F)$.*

Proof. We have the surjective map $c \rightsquigarrow [B(K, c)]$ of the group of reduced Brauer factor sets with values in E^* onto $\text{Br}(K/F)$. Now let $c^{(1)}$ and $c^{(2)}$ be reduced Brauer factor sets. Then it follows from Theorem 2.4.6 that $B(K, c^{(1)}) \otimes_F B(K, c^{(2)}) \sim B(K, c^{(1)} c^{(2)})$. This implies that $\text{Br}(K/F)$ is a subgroup of $\text{Br}(F)$ and $c \rightsquigarrow [B(K, c)]$ is a homomorphism of the group of reduced Brauer factor sets onto $\text{Br}(K/F)$. By Theorem 2.4.1, the kernel of this

homomorphism is the group of reduced $c \sim 1$. Hence $\text{Br}(K/F) \simeq H^2(K/F)$. \square

We also have the following generalization of the theorem of Speiser-Noether that $H^1(G, E^*) = 1$ for G the Galois group of E/F .

Theorem 2.5.12. *Let K be a finite dimensional commutative separable algebra over F , E/F a splitting field for K/F , $M = \{\alpha\}$ the set of homomorphisms of K/F into E/F . Let $(\alpha, \beta) \rightsquigarrow b(\alpha, \beta)$ be a homogeneous map of $M \times M$ into E^* such that*

$$b(\alpha, \beta)b(\beta, \gamma) = b(\alpha, \gamma) \quad (2.5.13)$$

for $\alpha, \beta, \gamma \in M$. Then there exists an invertible $a \in K$ such that

$$b(\alpha, \beta) = (\alpha a)(\beta a)^{-1}. \quad (2.5.14)$$

Proof. Consider the Brauer algebra $B(K, 1)$ which is the F -space of homogeneous maps of $M \times M$ into E with multiplication defined by $\ell\ell'(\alpha, \beta) = \sum_{\gamma \in M} \ell(\alpha, \gamma)\ell'(\gamma, \beta)$. For $k \in K$ we define a homogeneous map k' of $M \times M$ into E by $k'(\alpha, \alpha) = \alpha k$, $k'(\alpha, \beta) = 0$ if $\alpha \neq \beta$. Then $k \rightsquigarrow k'$ is a homomorphism of K into $B(K, 1)$. This is a monomorphism since $K \otimes_F E = Ee_1 \oplus \cdots \oplus Ee_n$ where the e_i are orthogonal idempotents and for any $k \in K$, $k = \sum (\alpha_i k) e_i$ where $\alpha_i k \in E$. Then $\alpha_i \in M$ and if $\alpha_i k = 0$ for all i , $k = 0$. Thus we can identify K with its image in $B(K, 1)$ and write k for k' . Then $B(K, 1)^K = K$ by Theorem 2.5.9. We now consider the map $\eta : \ell \rightsquigarrow \ell'$ where $\ell'(\alpha, \beta) = \ell(\alpha, \beta)b(\alpha, \beta)$ for $\ell \in B(K, 1)$. The condition (2.5.13) implies that η is an automorphism of $B(K, 1)$. Moreover, (2.5.13) gives $b(\alpha, \alpha)^2 = b(\alpha, \alpha)$ so $b(\alpha, \alpha) = 1$. Hence $\eta a = a$ for $a \in K$. It follows from the Skolem-Noether theorem and $B(K, 1)^K = K$ that there exists an invertible $a \in K$ such that $\eta = I_a$, the inner automorphism $x \rightsquigarrow axa^{-1}$. Now let v be defined by $v(\alpha, \beta) = 1$ for all α, β . Then v is homogeneous and $v' = \eta v$ satisfies $v'(\alpha, \beta) = b(\alpha, \beta)$. Since $(ava^{-1})(\alpha, \beta) = (\alpha a)(\beta a)^{-1}$ we have $b(\alpha, \beta) = (\alpha a)(\beta a)^{-1}$ for $\alpha, \beta \in M$. \square

2.6. Crossed Products

We shall now specialize to the case $E = K$, $M = G = \text{Gal } E/F$ in the foregoing considerations. In this case one has the crossed product representation, due to Emmy Noether, of a central simple algebra A containing E and having degree $n = [E : F]$. Let $\sigma \in G$. Then σ can be extended to an inner automorphism I_{u_σ} of A . By Theorem 2.5.9, $A^E = E$. Hence the element u_σ is determined up to a multiplier in E^* . Moreover, since $I_{u_\sigma} I_{u_\tau}$ and $I_{u_\sigma u_\tau}$ for $\sigma, \tau \in G$ have the same restriction $\sigma\tau$ to E , we have $u_\sigma u_\tau = k_{\sigma, \tau} u_{\sigma\tau}$, $k_{\sigma, \tau} \in E^*$. Also $u_\sigma a u_\sigma^{-1} = \sigma a$, $a \in E$. Thus we have

$$u_\sigma a = (\sigma a) u_\sigma, \quad u_\sigma u_\tau = k_{\sigma, \tau} u_{\sigma\tau} \quad (2.6.1)$$

for $a \in E$, $\sigma, \tau \in G$. The associativity $(u_\sigma u_\tau)u_\rho = u_\sigma(u_\tau u_\rho)$ gives the relations

$$k_{\sigma,\tau} k_{\sigma\tau,\rho} = k_{\sigma,\tau\rho} (\sigma k_{\tau,\rho}), \quad \sigma, \tau, \rho \in G. \quad (2.6.2)$$

It is clear from (2.6.1) that the E -subspace $\sum_{\sigma \in G} E u_\sigma$ is a subalgebra. On the other hand, it is easily seen by a Dedekind independence argument that the u_σ are linearly independent over E . Hence $[\Sigma E u_\sigma : E] = |G| = n$ and hence $[\Sigma E u_\sigma : F] = n^2 = [A : F]$. Thus

$$A = \Sigma E u_\sigma \quad (2.6.3)$$

We now consider the converse in which we begin with the Galois extension field E/F and the Galois group G . Then a map k of $G \times G$ into E^* : $(\sigma, \tau) \rightsquigarrow k_{\sigma,\tau}$ is called a *Noether factor set* if (2.6.2) holds. We form the (left) vector space over E with base $\{u_\sigma | \sigma \in G\}$ and we define a product in $A = \Sigma E u_\sigma$ by

$$(\Sigma a_\sigma u_\sigma)(\Sigma b_\tau u_\tau) = \sum_{\sigma, \tau} k_{\sigma,\tau} a_\sigma (\sigma b_\tau) u_{\sigma\tau}. \quad (2.6.4)$$

Then (2.6.2) implies that this is associative. Moreover, if we put $\sigma = \tau = 1$ and $\tau = \rho = 1$ successively in (2.6.2) we obtain

$$k_{1,\rho} = k_{1,1} \quad , \quad k_{\sigma,1} = \sigma k_{1,1} \quad (2.6.5)$$

which imply that $1 = k_{11}^{-1} u_1$ is the unit of A . Moreover, A is a vector space over $F \subset E$ and we have

$$\alpha(xy) = (\alpha x)y = x(\alpha y) \quad (2.6.6)$$

for $x, y \in A, \alpha \in F$. Thus A is an algebra over F (associative with 1). This is called the *crossed product of E with G and Noether factor set k* and is denoted as $A = (E, G, k)$. The result we proved above can now be stated as

Theorem 2.6.7. *If A is a central simple algebra containing E and the degree of A is $n = [E : F]$ then A is a crossed product (E, G, k) .*

It is quite easy to prove directly the converse that any crossed product is central simple over F of degree $n = [E : F]$. We shall obtain this result by establishing the connection between crossed products and Brauer algebras. We note first that if we replace u_1 by 1 we may assume that the Noether factor set is *normalized* in the sense that $k_{1,\sigma} = 1 = k_{\sigma,1}, \sigma \in G$. Then we have

Theorem 2.6.8. *If k is a normalized Noether factor set then c defined by*

$$c(\rho, \sigma, \tau) = \rho k_{\rho^{-1}\sigma, \sigma^{-1}\tau} \quad (2.6.9)$$

is a reduced Brauer factor set and $(E, G, k) \simeq B(E, c)$. Conversely, if c is a reduced Brauer factor set then

$$k_{\sigma,\tau} = c(1, \sigma, \sigma\tau) \quad (2.6.10)$$

defines a normalized Noether factor set and $B(E, c) \simeq (E, G, k)$.

Proof. First, let k be a normalized Noether factor set. Then $(E, G, k) = \{\Sigma a_\sigma u_\sigma \mid a_\sigma \in E\}$ and we have

$$\begin{aligned} (\Sigma a_\sigma u_\sigma)(\Sigma b_\tau u_\tau) &= \sum_{\sigma,\tau} k_{\sigma,\tau} a_\sigma (\sigma b_\tau) u_{\sigma\tau} \\ &= \left\{ \sum_{\tau\delta=\sigma} k_{\tau,\delta} a_\tau (\tau b_\delta) \right\} u_\sigma \\ &= \sum_{\sigma} \left\{ \sum_{\tau} k_{\tau,\tau^{-1}\sigma} a_\tau (\tau b_{\tau^{-1}\sigma}) \right\} u_\sigma. \end{aligned} \quad (2.6.11)$$

Now the element $\Sigma a_\sigma u_\sigma$ of (E, G, k) can be identified with the map $f : \sigma \rightsquigarrow a_\sigma$ of G into K . In this way $(E, G, k) = \{f \mid G \rightarrow E\}$ with the usual addition and multiplication by elements of F and with multiplication defined by

$$(fg)(\sigma) = \sum_{\tau} k_{\tau,\tau^{-1}\sigma} a_\tau (\tau b_{\tau^{-1}\sigma}). \quad (2.6.12)$$

The unit of (E, G, k) is now the map 1 such that $1 \rightsquigarrow 1$ and $\sigma \rightsquigarrow 0$ if $\sigma \neq 1$.

If k is a normalized Noether factor set then direct verification shows that c defined by (2.6.9) is a Brauer factor set, so we can define the Brauer algebra $B(E, c)$ as the set of homogeneous maps of $G \times G$ into E with the usual addition and multiplication by elements of F and multiplication defined by (2.5.7). Now for $f \in (E, G, k)$ we define $\xi f = \ell$ by

$$\ell(\sigma, \tau) = \sigma f(\sigma^{-1}\tau), \quad \sigma, \tau \in G. \quad (2.6.13)$$

Then $\ell(\rho\sigma, \rho\tau) = \rho\ell(\sigma, \tau)$ so $\xi f = \ell \in B(E, c)$ and $\xi : (E, G, k) \rightarrow B(E, c)$. Now ξ is bijective since if we define $\eta : B(E, c) \rightarrow (E, G, k)$ by $\eta\ell = f$ where

$$f(\sigma) = \ell(1, \sigma) \quad (2.6.14)$$

then $(\eta\xi)f = f$ for $f \in (E, G, k)$ and $(\xi\eta)\ell = \ell$ for $\ell \in B(E, c)$. It is clear that ξ is a vector space (over F) isomorphism. Now let $f, g \in (E, G, k)$. Then

$$(\xi f)(\xi g)(\sigma, \tau) = \sum_{\rho} \sigma f(\sigma^{-1}\rho) \sigma k_{\sigma^{-1}\rho, \rho^{-1}\tau} \rho g(\rho^{-1}\tau)$$

and

$$\begin{aligned} (\xi f g)(\sigma, \tau) &= \sigma \left(\sum_{\rho} k_{\rho, \rho^{-1}\sigma^{-1}\tau} f(\rho) \rho g(\rho^{-1}\sigma^{-1}\tau) \right) \\ &= \sigma \left(\sum_{\rho} k_{\sigma^{-1}\rho, \rho^{-1}\tau} f(\sigma^{-1}\rho) \rho g(\rho^{-1}\tau) \right). \end{aligned}$$

Hence $(\xi f)(\xi g) = \xi f g$ and ξ is an algebra isomorphism of (E, G, k) onto $B(E, c)$.

Direct verification shows that if c is a Brauer factor set then k defined by (2.6.10) is a Noether factor set and the map $c \rightsquigarrow k$ is the inverse of the map $k \rightsquigarrow c$ defined before. Hence if we are given $B(E, c)$ and we form (E, G, k) where $c \rightsquigarrow k$ then $(E, G, k) \simeq B(E, c)$.¹ \square

The Noether factor sets form a group under multiplication which contains the subgroup of factor sets of the form

$$(\sigma, \tau) \rightsquigarrow \ell_\sigma(\sigma \ell_\tau) \ell_{\sigma\tau}^{-1} \quad (2.6.15)$$

where $\sigma \rightsquigarrow \ell_\sigma$ is any map of G into E^* . The factor group is the cohomology group $H^2(G, E^*)$. As usual, we write $k \sim 1$ if k is in the subgroup defined by (2.6.13) and $k \sim k'$ if k and k' differ by an element of this subgroup.

We now observe that the map $k \rightsquigarrow c$ is an isomorphism of the group of Noether factor sets onto the group of Brauer factor sets. If ℓ is any map of G into E^* then $\ell(\sigma, \tau) = \sigma \ell(\sigma^{-1} \tau)$ is a homogeneous map of $G \times G$ into E^* . It follows that if $k \rightsquigarrow c$ in our homomorphism then $k \sim 1$ if and only if $c \sim 1$. Hence we have an induced isomorphism of $H^2(G, E^*)$ onto $H^2(E/F)$. This isomorphism together with Theorem 2.6.8 permit us to carry over the results of Sections 2.4 and 2.5 to Noether factor sets and crossed products. We obtain in this way the classical result of Emmy Noether:

Theorem 2.6.16. *Let E/F be a Galois extension with group G . Then*

- (i) *The crossed product $(E, G, k) \sim 1$ if and only if $k \sim 1$.*
- (ii) *$(E, G, k_1) \otimes_F (E, G, k_2) \sim (E, G, k_1 k_2)$.*
- (iii) *Let $[k]$ denote the element of $H^2(G, E^*)$ determined by k . Then $[k] \rightsquigarrow [(E, G, k)]$ is an isomorphism of $H^2(G, E^*)$ onto $\text{Br}(E/F)$.* \square

We now assume E/F is cyclic. Let σ be a generator of G and put $u = u_\sigma$. Then $u^i(u_{\sigma^i})^{-1}$ centralizes E ; hence $u^i = \ell_i u_{\sigma^i}$ where $\ell_i \in E^*$. We can replace u_{σ^i} by u^i , $0 \leq i \leq n-1$. This replaces the factor set k by k' where

$$k'_{\sigma^i, \sigma^j} = \begin{cases} 1 & \text{if } 0 \leq i+j \leq n-1 \\ \gamma & \text{if } i+j \geq n \end{cases} \quad (2.6.17)$$

and $\gamma \in E^*$. The crossed product A is generated by E and u and every element of A can be written in one and only one way as

$$a_0 + a_1 u + \cdots + a_{n-1} u^{n-1}, \quad a_i \in E. \quad (2.6.18)$$

We have the relations

$$ua = (\sigma a)u, \quad u^n = \gamma \quad (2.6.19)$$

if $a \in E$. Since u^n commutes with u and with every element of E^* , u^n is in the center F of A . Hence $\gamma \in F^*$. Thus we see that A is the cyclic algebra (E, σ, γ) .

¹ The foregoing proof is more direct than the one given in Jacobson [83₁]. I am indebted to Mr. Guo Li for pointing it out to me.

It is readily seen that if k' is defined by (2.6.10) then $k' \sim 1$ if and only if $\gamma = N(\ell)$ for $\ell \in E^*$. This permits the specialization of the main theorem on crossed products (2.6.16) to the following theorem on cyclic algebras.

Theorem 2.6.20.

- (i) *The cyclic algebra $(E, \sigma, \gamma) \sim 1$ if and only if $\gamma = N_{E/F}(\ell)$ for some $\ell \in E^*$.*
- (ii) *$(E, \sigma, \gamma_1) \otimes_F (E, \sigma, \gamma_2) \sim (E, \sigma, \gamma_1 \gamma_2)$.*
- (iii) *Let $N(E^*) = \{N_{E/F}(\ell), \ell \in E^*\}$. Then the map $\gamma N(E^*) \rightsquigarrow [(E, \sigma, \gamma)]$ is an isomorphism of $F^*/N(E^*)$ with $\text{Br}(E/F)$.*

The result just indicated shows that cyclic algebras can be regarded as special cases of crossed products. We shall now show that certain crossed products can be regarded as generalized cyclic algebras. We consider a crossed product $A = (E, G, k)$ and we suppose $H \triangleleft G$ and G/H is cyclic. Let τ be an element of G such that the coset τH generates G/H . Then any element of G has the form $\sigma \tau^i$ where $\sigma \in H$ and $0 \leq i < r = |G/H|$. Moreover, $\tau^r \in H$. Let D be the subalgebra of A generated by E and the $u_\sigma, \sigma \in H$. If $F' = \text{Inv } H$ then F' is the center of D . It is clear that D as algebra over F' is the crossed product (E, H, k') where $k' = \{k_{\sigma, \sigma'} | \sigma, \sigma' \in H\}$. Since $H \triangleleft G, \tau \sigma \tau^{-1} \in \sigma'$ if $\sigma \in H$. Hence if we put $u = u_\tau$ then the inner automorphism I_u stabilizes D . Let $\tilde{\sigma} = I_u | D$. Then we have the relation $ua = (\tilde{\sigma}a)u$, $a \in D$. Moreover, $u^r = \ell u_{\tau^r}$ where $\ell \in E^*$ and since $\tau^r \in H$ we have $u^r = b \in D$. It follows that if D is a division algebra then A is a generalized cyclic algebra $(D, \tilde{\sigma}, b)$. In particular this is the case if A is a division algebra.

2.7. The Exponent of a Central Simple Algebra

If A is a central simple algebra over F then $A = M_r(D)$ where D is a central division algebra. If $[D : F] = d^2$ then we have called d the *index* of A (or of $[A]$). We shall now prove that $\text{Br}(F)$ is a torsion group by proving

Theorem 2.7.1. *If d is the index of A then $[A]^d = 1$.*

Proof. Let E be a finite dimensional Galois splitting field for A . By replacing A by another element of $[A]$ we may assume that $A = M_r(D) = (E, G, k)$. Now A can be identified with $\text{End}_{D^0}(V)$ where V is an r -dimensional vector space over D^0 . Since A contains the field E , V can also be regarded as a vector space over E . If $[E : F] = n$ then $[V : F] = [V : E][E : F] = n[V : E]$. Also $[V : F] = [V : D^0][D^0 : F] = rd^2$ and $[A : F] = n^2 = r^2 d^2$ so $n = rd$. Hence $n[V : E] = nd$ and $[V : E] = d$. If $\{u_\sigma | \sigma \in G\}$ is the base for $A = (E, G, k)$ such that (2.6.1) holds then the first of these relations shows that u_σ is a σ -semi-linear transformation of V/E . Now let (x_1, x_2, \dots, x_d) be a base for V/E and write

$$u_\sigma x_i = \sum_{j=1}^d M_{ji}(\sigma) x_j. \quad (2.7.2)$$

Then $M_\sigma = (M_{ij}(\sigma))$ is the matrix of u_σ relative to (x_1, x_2, \dots, x_d) . The relations $u_\sigma u_\tau = k_{\sigma, \tau} u_{\sigma\tau}$ imply the matrix relations

$$M_\sigma(\sigma M_\tau) = k_{\sigma, \tau} M_{\sigma\tau}. \quad (2.7.3)$$

Let $\mu_\sigma = \det M_\sigma$. Then we have

$$\mu_\sigma(\sigma \mu_\tau) = k_{\sigma, \tau}^d \mu_{\sigma\tau}. \quad (2.7.4)$$

Since u_σ is invertible, $\mu_\sigma \neq 0$ and hence (2.7.4) gives $k_{\sigma, \tau}^d = \mu_\sigma(\sigma \mu_\tau) \mu_{\sigma\tau}^{-1}$ and so $k^d \sim 1$. Hence $A^d \sim 1$ by (2.6.9). \square

The order of $\{A\}$ in $\text{Br}(F)$ is called the *exponent* $e(A)$ of A . This is the smallest positive integer e such that $\overbrace{A \otimes A \otimes \dots \otimes A}^e \sim 1$. The preceding theorem implies that the exponent is a factor of the index. We shall now show that these two integers have the same prime factors.

Theorem 2.7.5. *If p is a prime dividing the index of A then p divides the exponent of A .*

Proof. Suppose $p \mid d$. We may assume $A = (E, G, k) = M_r(D)$ where $[D : F] = d^2$. Then $p \mid n = rd$ and hence $p \mid |G|$, $G = \text{Gal } E/F$. Let H be a Sylow p -subgroup of G , K the subfield of E such that $\text{Gal } E/K = H$. Then $[E : K] = p^m$ and $p \nmid [K : F]$. Consider A_K . This is a central simple algebra over K and since $d \nmid [K : F]$, K is not a splitting field for A so $A_K \not\sim 1$. On the other hand, E/K is a splitting field for A_K so the index of A_K has the form $p^s \neq 1$. Since $A_K \not\sim 1$, $e(A_K) \neq 1$ and since $e(A_K) \mid p^s$ we see that $p \mid e(A_K)$. Since the map $B \mapsto B_K$ is a homomorphism of $\text{Br}(F)$ into $\text{Br}(E)$ it follows that $p \mid e(A)$. \square

We shall now use the results on exponents to prove that any central division algebra is a tensor product of central division algebras of prime power degrees. We require the

Lemma 2.7.6. *Let D_1 and D_2 be finite dimensional division algebras. Assume D_1 is central and $([D_1 : F], [D_2 : F]) = 1$. Then $D_1 \otimes_F D_2$ is a division algebra.*

Proof. $D_1 \otimes_F D_2$ is simple (Corollary 2, p. 219 of BA II). Hence $D_1 \otimes_F D_2 = M_r(D)$ where D is a division algebra. Now $M_r(D)$ is a direct sum of r minimal left ideals I_1, I_2, \dots, I_r and these are isomorphic modules for $M_r(D)$. Hence they are also isomorphic as D_i -modules. Then $[D_i : F] = [M_r(D) : D_j]_l$ for $j \neq i$ is divisible by r . Since $([D_1 : F], [D_2 : F]) = 1$ this implies that $r = 1$ and so $D_1 \otimes_F D_2 = D$. \square

Theorem 2.7.7. *Let D be a central division algebra of degree $d = p_1^{k_1} \cdots p_s^{k_s}$, p_i distinct primes. Then $D \simeq D_1 \otimes D_2 \otimes \cdots \otimes D_s$ where D_i is a central division algebra of degree $p_i^{k_i}$.*

Proof. Let e be the exponent of D . Then $e = e_1 e_2 \cdots e_s$ where $e_i = p_i^{m_i}$, $0 < m_i \leq k_i$. The cyclic group $\langle [D] \rangle$ has order e so $[D] = [D_1][D_2] \cdots [D_s]$ where D_i is a central division algebra of exponent e_i and hence of degree $p_i^{k'_i}$, $k'_i \geq m_i$. By 2.7.6, $D_1 \otimes_F D_2 \otimes_F \cdots \otimes_F D_s$ is a division algebra and its degree is $p_1^{k'_1} \cdots p_s^{k'_s}$. Hence $D \simeq D_1 \otimes \cdots \otimes D_s$ and the degree of D is $p_1^{k'_1} \cdots p_s^{k'_s}$. Thus $k_i = k'_i$, $1 \leq i \leq s$. \square

2.8. Central Division Algebras of Prescribed Exponent and Degree

We have seen in the last section that if D is a central division algebra of degree d and exponent e then

- (i) $e \mid d$
- (ii) every prime factor of d is a factor of e .

We shall now show that if d and e are positive integers satisfying these conditions then there exists a D having degree d and exponent e . The construction we shall give is one given by Brauer in [33].

We assume first only condition (ii) on d and e .

Let P be a field of characteristic 0 such that

1. P contains a primitive e -th root ε of 1.
2. $\lambda^d - \varepsilon$ is irreducible in $P[\lambda]$.

The following lemma gives an example of a field satisfying these conditions and gives some properties of any P satisfying the conditions.

Lemma 2.8.1.

- (1) *The cyclotomic field Λ_e over \mathbf{Q} of e -th roots of 1 satisfies 1. and 2.*
- (2) *If P satisfies the conditions 1. and 2. and p is a prime divisor of d then P contains no primitive pe -th root of 1.*
- (3) *If P satisfies the conditions 1. and 2. above and E is an extension field of P that contains an element η such that $\eta^d = \varepsilon$ then η is a primitive de -th root of 1.*

Proof. (1) We have $[\Lambda_e : \mathbf{Q}] = \phi(e)$ and $[\Lambda_{de} : \mathbf{Q}] = \phi(de)$. The condition (ii) implies that $\phi(de) = d\phi(e)$. Hence $[\Lambda_{de} : \Lambda_e] = d$. Let ε be a primitive e -th root of 1, ε' a primitive de -th root of 1. Since ε'^d is also a primitive e -th root of 1 we have $\Lambda_e = \mathbf{Q}(\varepsilon'^d)$ and $\lambda^d - \varepsilon'^d$ is the minimum polynomial of ε' over Λ_e . Hence $\lambda^d - \varepsilon'^d$ is irreducible in $\Lambda_e[\lambda]$. Since ε and ε'^d are primitive e -th

roots of 1 there is an automorphism of Λ_e sending ε'^d into ε . Hence $\lambda^d - \varepsilon$ is irreducible in $\Lambda_e[\lambda]$.

(2) Suppose P satisfies the conditions 1. and 2. and P contains a primitive pe -th root ε' of 1. Then $P \supset \Lambda_{pe} \supset \Lambda_e$ and we have an automorphism of Λ_e sending ε'^p into ε . This can be extended to an automorphism of Λ_{pe} . Since $\lambda^p - \varepsilon'^p$ is reducible in $\Lambda_{pe}[\lambda]$ the same is true of $\lambda^p - \varepsilon$. Hence $\lambda^p - \varepsilon$ is reducible in $P[\lambda]$ and, consequently, $\lambda^d - \varepsilon$ is reducible in $P[\lambda]$ contrary to condition 2.

(3) We have $P \supset \Lambda_e$ and $E \supset \Lambda_e(\eta)$, $\Lambda_e(\eta) \subset \Lambda_{de}$ and $[\Lambda_e(\eta) : \Lambda_e] = d = [\Lambda_{de} : \Lambda_e]$. Hence $\Lambda_{de} = \Lambda_e(\eta)$. Let ε' be a primitive de -th root of 1. As before, we have an automorphism of Λ_e sending ε'^d into ε and this can be extended to an automorphism of Λ_{de} sending ε' into η . Hence η is a primitive de -th root of 1. \square

Now let P satisfy 1. and 2. and let $E = P(x_1, \dots, x_d)$ the field of rational expressions in indeterminates x_i over P . Let σ be the automorphism of E/P permuting the x_i cyclically. Let $F = \text{Inv}\langle\sigma\rangle$ so E/F is cyclic with Galois group $G = \langle\sigma\rangle$. Hence we can form the cyclic algebra $A/F = (E, \sigma, \varepsilon)$ where ε is as in 1. and 2. We shall prove

Theorem 2.8.2. $A = (E, \sigma, \varepsilon)$ is a division algebra.

For the proof we shall need some results on the action of σ in the polynomial ring $R = P[x_1, \dots, x_d]$. For the present we drop the assumption on the existence of ε and assume only that $\text{char } P \nmid d$. We note first that if $f \in R$ then $N(f) \equiv f(\sigma f) \cdots (\sigma^{d-1} f) \in S = F \cap R$ and if $f \neq 0$ then $N(f) \neq 0$ and $f \mid N(f)$ in R . It follows that if $f \in E$ then there is a $g \neq 0$ in S such that $gf \in R$. If $t \mid d$ we put

$$E^{(t)} = \text{Inv}\langle\sigma^t\rangle, \quad R^{(t)} = E^{(t)} \cap R. \quad (2.8.3)$$

Then $E = E^{(d)}$, $F = E^{(1)}$, $R = R^{(d)}$, $S = R^{(1)}$.

Let $V = \sum_1^d P x_i$. Then V is stabilized by σ so V is a $P[\sigma]$ -module. Since σ is a root of $\lambda^d - 1$ and this polynomial is a product of distinct prime polynomials, $V = V_i \oplus \cdots \oplus V_r$ where the V_i are irreducible $P[\sigma]$ -modules. Let $\lambda_i \in \mathbf{N}$ and put

$$V_{(\lambda_1, \dots, \lambda_r)} = V_1^{\lambda_1} V_2^{\lambda_2} \cdots V_r^{\lambda_r} \subset R. \quad (2.8.4)$$

Then R is graded by the $V_{(\lambda_1, \dots, \lambda_r)}$:

$$\begin{aligned} R &= \bigoplus V_{(\lambda_1, \dots, \lambda_r)} \\ (\lambda_1, \dots, \lambda_r) &\in \mathbf{N}^{(r)} \\ V_{(\lambda_1, \dots, \lambda_r)} V_{(\mu_1, \dots, \mu_r)} &\subset V_{(\lambda_1 + \mu_1, \dots, \lambda_r + \mu_r)} \end{aligned} \quad (2.8.5)$$

We shall call this a σ -grading of R . The elements of $V_{(\lambda_1, \dots, \lambda_r)}$ are said to be *homogeneous of degree* $(\lambda_1, \dots, \lambda_r)$.

Evidently $\sigma V_{(\lambda_1, \dots, \lambda_r)} = V_{(\lambda_1, \dots, \lambda_r)}$. This implies that if $t \mid d$ then

$$R^{(t)} = \Sigma V_{(\lambda_1, \dots, \lambda_r)}^{(t)}, \quad V_{(\lambda_1, \dots, \lambda_r)}^{(t)} = R^{(t)} \cap V_{(\lambda_1, \dots, \lambda_r)}. \quad (2.8.6)$$

This is equivalent to: if $a \in R^{(t)}$ and $a = \Sigma a_{(\lambda_1, \dots, \lambda_r)}$ where $a_{(\lambda_1, \dots, \lambda_r)} \in V_{(\lambda_1, \dots, \lambda_r)}$ then $a_{(\lambda_1, \dots, \lambda_r)} \in R^{(t)}$.

We shall need the following

Lemma 2.8.7. *Suppose $t \mid d$ and $t' \mid t$ and assume P contains a primitive d/t' -th root of unity. Then for any $(\lambda_1, \dots, \lambda_r)$ there exists a homogeneous element $g \neq 0$ in $R^{(t)}$ such that*

$$gV_{(\lambda_1, \dots, \lambda_r)}^{(t)} \subset R^{(t')}. \quad (2.8.8)$$

Proof. We have $(\sigma^{t'})^{d/t'} = 1$ so the condition that P contains a primitive d/t' -th root of 1 implies that the characteristic roots of $\sigma^{t'} \mid V$ are contained in P . Since V_i is an irreducible module it follows that $\sigma^{t'} \mid V_{=c_i 1_{V_i}}$. Then $\sigma^{t'} \mid V_{(\lambda_1, \dots, \lambda_r)} = c_1^{\lambda_1} \cdots c_r^{\lambda_r} 1_{V_{(\lambda_1, \dots, \lambda_r)}}$. Now the c_i are d/t' -th roots of unity and they generate the group of d/t' -th roots of unity. Otherwise, we have $(\sigma \mid R)^h = 1$ for $h < d$ and hence $\sigma^h = 1$ contrary to the fact that σ has order d in E . Now let $f \in V_{(\lambda_1, \dots, \lambda_r)}^{(t)}$. Then $\sigma^{t'} f = cf$, for $c = c_1^{\lambda_1} \cdots c_r^{\lambda_r}$, and $f = \sigma^t f = (\sigma^{t'})^{t/t'} f = c^{t/t'} f$ so $c^{t/t'} = 1$. Also we have $c^{-1} = c_1^{\mu_1} \cdots c_r^{\mu_r}$ so if we choose $g \neq 0$ in $V_{(\mu_1, \dots, \mu_r)}$ then $\sigma^{t'} g = c^{-1} g$ and $\sigma^t g = (\sigma^{t'})^{t/t'} g = (c^{-1})^{t/t'} g = g$. Thus $g \in R^{(t)}$ and $\sigma^{t'}(gf) = c^{-1} c g f = g f$. Hence $g f \in R^{(t')}$. The argument shows that this holds for every $f \in V_{(\lambda_1, \dots, \lambda_r)}^{(t)}$. Hence we have (2.8.8). \square

Proof of Theorem 2.8.2. Let $u \in A = (E, \sigma, \varepsilon)$ satisfy

$$ua = (\sigma a)u, \quad a \in E, \quad u^d = \varepsilon. \quad (2.8.9)$$

Then the elements of A can be written in one and only one way in the form $\sum_{i=0}^{d-1} a_i u^i$, $a_i \in E$. We have assumed that $\lambda^d - \varepsilon$ is irreducible in $P[\lambda]$. Hence $\lambda^d - \varepsilon$ is irreducible in $R[\lambda] = P[x_1, \dots, x_r, \lambda]$ and hence in $E[\lambda]$. A fortiori $\lambda^d - \varepsilon$ is irreducible in $F[\lambda]$ so $F[u]$ is a subfield of A . Since $[F[u] : F] = d$ this is a maximal subfield and the centralizer $A^{F[u]} = F[u]$. By Lemma 2.8.1 (3), u is a primitive de -th root of unity.

Now let $t \mid d$ and consider the subfield $F[u^t]$ of $F[u]$. Since $\lambda^d - \varepsilon$ is irreducible in $F[\lambda]$ (or in $E[\lambda]$), $\lambda^{d/t} - \varepsilon$ is irreducible in $F[\lambda](E[\lambda])$ since u^t is a root of $\lambda^{d/t} - \varepsilon$, $(F[u^t] : F) = d/t$. Also u^t is a primitive de/t -th root of 1. Let $A_t = A^{F[u^t]}$. By the double centralizer theorem for central simple algebras (Theorem 4.10, p. 222 of BA II), $F[u^t]$ is the center of A_t . It is clear from 2.8.9 that

$$\begin{aligned} A_t &= \left\{ \sum_{j=0}^{d-1} a'_j u^j \mid a'_j \in E^{(t)} \right\} \\ &= \left\{ \sum_{i=0}^{t-1} a_i u^i \mid a_i \in E^{(t)}[u^t] \right\}. \end{aligned} \quad (2.8.10)$$

Now $E^{(t)}[u^t]$ is a field since u^t is a root of $\lambda^{d/t} - \varepsilon$ which is irreducible in $E[\lambda]$ and hence in $E^{(t)}[\lambda]$. The automorphism I_u stabilizes $E^{(t)}[u^t]$ and $\sigma_t = I_u \mid E^{(t)}[u^t]$ restricts to σ on $E^{(t)}$. Hence σ_t has order t and

$$A_t = (E^{(t)}[u^t], \sigma_t, u^t) \quad (2.8.11)$$

as algebra over $F[u^t]$.

Now $A_1 = F[u]$ and $A_d = A$. We shall now prove by induction on t that every A_t is a division algebra. Thus we assume every $A_{t'}, t' < t$, is a division algebra. Suppose A_t is not a division algebra. Then $t > 1$ and A_t contains zero divisors $\neq 0$. Let p be a prime divisor of t and put $t' = t/p$. We shall show that the existence of zero divisors $\neq 0$ in A_t implies the existence of such zero divisors in $A_{t'}$. This will contradict the hypothesis on $A_{t'}$ and prove the theorem.

Now let $a = \sum_0^{t-1} a_i u^i, b = \sum_0^{t-1} b_i u^i$ where $a_i, b_i \in E^{(t)}[u^t]$ satisfy $a \neq 0, b \neq 0, ab = 0$. Since the $u_i, 0 \leq i \leq t-1$ are independent over $E^{(t)}[u^t]$, $ab = 0$ is equivalent to a system of polynomial equations in a_i and $\sigma_i^k b_i$ with coefficients in $P[u^t]$ and we are assuming that these are solvable for a_i not all 0 and b_i not all 0. We note also that if the a_i and b_i can be chosen in $E^{(t')}[u^t]$ then we shall have $a \neq 0, b \neq 0$ in $A_{t'}$ such that $ab = 0$.

We now replace P by $P[u^t]$ in the field considerations at the beginning of this section. If we write P for $P[u^t]$ then P contains a primitive de/t -th root of 1 and since $t' = t/p, de/t = de/t'p$ is a multiple of d/t' (since $p \mid e$ by condition (ii)). Hence P contains a primitive d/t' -th root of 1. We note that if we multiply the given a_i by a suitable non-zero element of S we may assume the $a_i \in R^{(t)}$. Similarly we may assume the $b_i \in R^{(t)}$. Next we can express the a_i and b_i as sums of homogeneous elements in the σ -grading. Moreover, we can order the degrees lexicographically and thus regard $\mathbf{N}^{(r)}$ as an ordered monoid. Let $(\lambda_1, \dots, \lambda_r)$ be the lowest degree of homogeneity of the non-zero homogeneous parts of all the a_i and let (μ_1, \dots, μ_r) have the same significance for the b_i . Then it is clear that if we replace each a_i by its homogeneous part of degree $(\lambda_1, \dots, \lambda_r)$ if there is one and by 0 otherwise, and we make the same type of replacement for the b_i then the equations giving $ab = 0$ are satisfied. Thus we may assume the a_i are homogeneous of the same degree $(\lambda_1, \dots, \lambda_r)$ and the b_i are homogeneous of the same degree (μ_1, \dots, μ_r) . Since P contains a primitive d/t' -th root of 1 we can apply Lemma 2.8.7 to obtain an element $g \neq 0$ in $R^{(t)}$ such that every $ga_i \in R^{(t')}$. Also if we apply the lemma and observe that g in this lemma can be replaced by $\sigma^k g$ for any k (since $\sigma V_{(\lambda_1, \dots, \lambda_r)}^{(t)} = V_{(\lambda_1, \dots, \lambda_r)}^{(t)}$ and $\sigma R^{(t)} = R^{(t')}$) we see that there exists an $h \neq 0$ in $R^{(t)}$ such that $bh \in A_{t'}$. We have $ga \neq 0, bh \neq 0$ and $(ga)(bh) = 0$ with $ga, bh \in A_{t'}$. This completes the proof. \square

We now assume both conditions (i) and (ii) on d and e and we prove

Theorem 2.8.12. $A = (E, \sigma, \varepsilon)$ has exponent e in $\text{Br}(F)$.

Proof. Let e' be the smallest positive integer such that $\varepsilon^{e'} = N(E^*)$. Since $\varepsilon^e = 1, e' \mid e$. The assertion is equivalent, by the result noted at the end of Section 2.7, to $e' = e$. Now suppose $\varepsilon^{e'} = N_{E/F}(h)$. We can write $h = f/g$ where $f, g \in R = P[x_1, \dots, x_d]$. Then

$$f(\sigma f) \cdots (\sigma^{d-1} f) = \varepsilon^{e'} g(\sigma g) \cdots (\sigma^{d-1} g). \quad (2.8.13)$$

We assume $\deg f$ minimal. If $\deg f > 0$ let q be an irreducible factor of f in R . Then $q \mid \sigma^i g$ for some i and $N_{E/F}(q) \mid N_{E/F}(g)$ in R . We can cancel $N_{E/F}(q)$ on both sides of (2.8.13) to obtain a relation (2.8.13) with f of lower degree. Hence $\deg f = 0$ and then $\deg g = 0$. Thus $\varepsilon^{e'} = N_{E/F}(h)$ with $h \in P$ and hence

$$\varepsilon^{e'} = h^d, \quad h \in P. \quad (2.8.14)$$

The order of $\varepsilon^{e'}$ in the multiplicative group P^* is e/e' . On the other hand, the order of h^d in P^* is $k/(d, k)$ where k is the order of h . Hence

$$k/(d, k) = e/e'. \quad (2.8.15)$$

The conditions (i) and (ii) on d and e and (2.8.15) imply that any prime dividing k divides e . Moreover, if k is divisible by a higher power of p than e then P^* contains a primitive pe -th root of 1 contrary to Lemma 2.8.1 (2). It now follows that $k \mid e$. Hence $k \mid d$ and $(d, k) = k$. Then $e \mid e'$, by (2.8.15). Thus $e' = e$. \square

2.9. Central Division Algebras of Degree ≤ 4 .

We shall prove that these algebras are crossed products. The result for degree $d = 2$ is folklore. For degree three it is due to Wedderburn and for degree four in the sharper form that any central division algebra of degree four contains a maximal subfield whose Galois group is $Z_2 \times Z_2$ (Z_k cyclic of order k), it is due to Albert [29].

$d = 2$. The quickest way of obtaining the result for degree two is to invoke the theorem that such an algebra D contains a maximal separable subfield E/F (Theorem 1.6.19). Such a field is Galois. In a more elementary fashion the “difficult” case of characteristic 2 can be settled by the following argument. Let $d \in D$ be inseparable. Then $d \notin F, d^2 \in F$. Choose $a \in D, a \notin F(d)$. Then $b = [da] \neq 0$ but $[db] = [d[da]] = [d^2a] = 0$. Put $c = ab^{-1}d$. Then $[dc] = d, dcd^{-1} = c + 1$. Then $dc^2d^{-1} = (dcd^{-1})^2 = (c + 1)^2 = c^2 + 1$. Hence $d(c^2 + c)d^{-1} = c^2 + c$ so $c^2 + c$ commutes with d and c . Since D is generated by d and c , $c^2 + c \in F$. Thus $c^2 + c = \gamma \in F$ which evidently implies that c is a separable element and $c \notin F$.

$d = 3$. We shall give Wedderburn’s proof (Wedderburn [21]) which is based on his factorization theorem for the minimum polynomial of an element of a central division algebra. This is the following

Theorem 2.9.1. *Let D be a finite dimensional central division algebra over a field F and let $a \in D$ and $f(\lambda) \in F[\lambda]$ be the minimum polynomial of a over F . Suppose $\deg f = m$. Then we have the factorization*

$$f(\lambda) = (\lambda - a_m)(\lambda - a_{m-1}) \cdots (\lambda - a_1) \quad (2.9.2)$$

in $D[\lambda]$ where $a_1 = a$ and the a_i are conjugates of a . Moreover, if $a \notin F$ then $m > 1$ and we may take

$$a_2 = [ya_1]a_1[ya_1]^{-1} \quad (2.9.3)$$

where y is any element of D that does not commute with a .

All but the last statement has been proved in Corollary 1.3.14. We shall now give Wedderburn's proof of 2.9.1 including the last statement. This is based on

Lemma 2.9.4. *Let D be a division ring and let $a \in D$. Suppose $(\lambda - a) \mid_r g(\lambda)f(\lambda)$ in $D[\lambda]$ but $(\lambda - a) \nmid_r f(\lambda) = b_0\lambda^m + b_1\lambda^{m-1} + \cdots + b_m$. Then $R = b_0a^m + b_1a^{m-1} + \cdots + b_m \neq 0$ and $(\lambda - RaR^{-1}) \mid_r g(\lambda)$.*

Proof. We have $f(\lambda) = Q(\lambda)(\lambda - a) + R$ where $R = b_0a^m + b_1a^{m-1} + \cdots + b_m$ (see (1.3.10)). Since $(\lambda - a) \nmid_r f(\lambda)$, $R \neq 0$. Now $g(\lambda)f(\lambda) = g(\lambda)Q(\lambda)(\lambda - a) + g(\lambda)R$ and since $(\lambda - a) \mid_r g(\lambda)f(\lambda)$, $(\lambda - a) \mid_r g(\lambda)R$. Then $(\lambda - RaR^{-1}) \mid_r g(\lambda)$. \square

We can now give the

Proof of Theorem 2.9.1. The result is clear if $a_1 = a \in F1$. Now suppose $a_1 \notin F1$. Then $m > 1$ and there exists a $y \in D$ such that $[ya_1] \neq 0$. Let y be any such element of D . Since $f(a_1) = 0$ we have $f(\lambda) = f_1(\lambda)(\lambda - a_1)$ and $f(\lambda) = yf(\lambda)y^{-1} = yf_1(\lambda)y^{-1}(\lambda - ya_1y^{-1})$. Since $ya_1y^{-1} \neq a_1$, $R = ya_1y^{-1} - a_1 \neq 0$ and by 2.9.4, $\lambda - Rya_1y^{-1}R^{-1} \mid_r f_1(\lambda)$. Thus

$$f(\lambda) = f_2(\lambda)(\lambda - a_2)(\lambda - a_1) \quad (2.9.5)$$

where $a_2 = Rya_1y^{-1}R^{-1}$ where $R = ya_1y^{-1} - a_1$. Hence $a_2 = [ya_1]a_1[ya_1]^{-1}$. Now suppose we have

$$f(\lambda) = g_k(\lambda)(\lambda - a_k) \cdots (\lambda - a_2)(\lambda - a_1) \quad (2.9.6)$$

where $k < m$, the a_i are conjugates of a_1 and $a_2 = [ya_1]a_1[ya_1]^{-1}$. We claim there is a conjugate a'_{k+1} of a_1 such that $(\lambda - a'_{k+1}) \nmid_r f_k(\lambda)$ where $f_k(\lambda) = (\lambda - a_k) \cdots (\lambda - a_2)(\lambda - a_1)$. Otherwise, we have a monic polynomial $f_k(\lambda) \in D[\lambda]$ of degree $k < m$ such that $(\lambda - za_1z^{-1}) \mid_r f_k(\lambda)$ for all $z \neq 0$. We may assume k minimal. Then $(\lambda - a) \mid_r z^{-1}f_k(\lambda)z$ for all $z \neq 0$. This implies $z^{-1}f_k(\lambda)z = f_k(\lambda)$ for all $z \neq 0$ since if there is a $z_0 \neq 0$ such that $z_0^{-1}f_k(\lambda)z_0 \neq f_k(\lambda)$ then we have a monic polynomial $g(\lambda)$ of the form $b(z_0^{-1}f_k(\lambda)z_0 - f_k(\lambda))$ of degree $< k$ such that $(\lambda - a) \mid_r zg(\lambda)z^{-1}$ for all $z \neq 0$. This contradicts the minimality of k . On the other hand, if $z^{-1}f_k(\lambda)z = f_k(\lambda)$ for all $z \neq 0$ then

$f_k(\lambda) \in F[\lambda]$ and since $f_k(a_1) = 0$ we have a contradiction to the hypothesis that $f(\lambda)$ is the minimum polynomial of a_1 . Thus we have a conjugate a'_{k+1} of a_1 such that $(\lambda - a'_{k+1}) \nmid f_k(\lambda)$. Then, by the lemma, we have a conjugate a_{k+1} of a_1 such that $(\lambda - a_{k+1}) \mid_r g_k(\lambda)$. This establishes the inductive step that $f(\lambda) = g_{k+1}(\lambda)(\lambda - a_{k+1}) \cdots (\lambda - a_2)(\lambda - a_1)$ where the a_i are conjugates of a_1 and a_2 is as stated. \square

We shall call an element a of a central division algebra D *cyclic* if $F(a)$ is a cyclic subfield of D . Then we have

Proposition 2.9.7. *Let D be a central division algebra of prime degree p and let $a \in D$ have degree p . Then a is cyclic if and only if there exists a $y \in D$ such that $yay^{-1} \neq a$ and $[yay^{-1}, a] = 0$.*

Proof. Suppose first we have a y satisfying the foregoing conditions. Since a is of degree p , $F(a)$ is a maximal subfield, so the condition $[yay^{-1}, a] = 0$ implies that $yay^{-1} \in F(a)$ and hence $\sigma = I_y \mid F(a)$ is an automorphism of $F(a)$. Since $yay^{-1} \neq a, \sigma \neq 1_{F(a)}$. Since $[F(a) : F]$ is prime, $F = \text{Inv}(\sigma)$ and hence $F(a)$ is Galois over F with $\text{Gal } F(a)/F = \langle \sigma \rangle$. Conversely, suppose a is cyclic and $\text{Gal } F(a)/F = \langle \sigma \rangle$ then $\sigma a \neq a$ and we have a $y \in D$ such that $yay^{-1} = \sigma a$. Thus $yay^{-1} \neq a$ and $[yay^{-1}, a] = 0$. \square

We can now prove the key

Lemma 2.9.8. *Let D be a central division algebra of degree three over F and let a be a non-cyclic element of D . Then the minimum polynomial $f(\lambda) = \lambda^3 - \alpha_1\lambda^2 + \alpha_2\lambda - \alpha_3$ of a over F has a factorization*

$$f(\lambda) = (\lambda - a_3)(\lambda - a_2)(\lambda - a_1) \quad (2.9.9)$$

where $a_1 = a$,

$$c = [a_1a_2] = [a_2a_3] = [a_3a_1] \neq 0 \quad (2.9.10)$$

$$ca_i c^{-1} = a_{i+1} \quad (\text{indices reduced mod } 3) \quad (2.9.11)$$

$$c^3 = \gamma, \quad \gamma \in F. \quad (2.9.12)$$

Proof. Since $f(a_1) = 0$ for $a_1 = a$ we have $f(\lambda) = g(\lambda)(\lambda - a_1)$. We claim we can choose $y \in D$ so that $[[ya_1]a_1] \neq 0$. Otherwise, $i_{a_1}^2 = 0$ for the inner derivation $i_{a_1} = a_{1L} - a_{1R}$. Then $a_{1L}^2 a_{1R} + a_{1R}^2 = 0$. Since $a_1 \notin F, [F[a_1] : F] = 3$ so $1, a_1, a_1^2$ are linearly independent over F . Then the 9 linear transformations $a_{1L}^i a_{1R}^j, 0 \leq i, j \leq 2$, are linearly independent² This contradicts $a_{1L}^2 - 2a_{1L}a_{1R} + a_{1R}^2 = 0$.

² This is a special case of a general result on finite dimensional central simple algebras: If A is such an algebra over F and $\{a_1, \dots, a_r\}, \{b_1, \dots, b_s\}$ are two sets of linearly independent elements, then the rs linear transformations $a_{iL}b_{jR}, 1 \leq i \leq r, 1 \leq j \leq s$, are linearly independent. (See e.g., the proof of Theorem 4.6, p. 218 of BA II).

Now let y be an element such that $[[ya_1]a_1] \neq 0$. Then $ya_1y^{-1} \neq a_1$ and by Wedderburn's factorization theorem, $f(\lambda) = (\lambda - a_3)(\lambda - a_2)(\lambda - a_1)$ where $a_2 = [ya_1]a_1[ya_1]^{-1}$. Since $f(\lambda) \in F[\lambda]$ it is clear that the factors of $f(\lambda)$ can be permuted cyclically. Hence $(\lambda - a_2) \mid_r f(\lambda)$. On the other hand, $(\lambda - a_2) \nmid_r (\lambda - a_2)(\lambda - a_1)$. Otherwise, $(\lambda - a_2)(\lambda - a_1) = (\lambda - b)(\lambda - a_2)$. Comparison of the coefficients of λ shows that $b = a_1$. Then $a_1a_2 = a_2a_1$. Since $a_2 = Rya_1y^{-1}R^{-1}$ and a_1 is not cyclic, $Rya_1y^{-1}R^{-1} = a_1$ by 2.9.7. Then $[Ry, a_1] = 0$ and since $Ry = ya_1 - a_1y$, $[[ya_1]a_1] = 0$ contrary to the choice of y . Thus $(\lambda - a_2) \nmid_r (\lambda - a_2)(\lambda - a_1)$. It now follows from Lemma 2.9.4 that $\lambda - (a_2a_1 - a_1a_2)a_2(a_2a_1 - a_1a_2)^{-1} \mid_r (\lambda - a_3)$. Hence

$$a_3 = [a_2a_1]a_2[a_2a_1]^{-1}. \quad (2.9.13)$$

Next we use the relations

$$\begin{aligned} \alpha_2 &= a_3a_2 + a_3a_1 + a_2a_1 = a_1a_3 + a_1a_2 + a_3a_2 \\ &= a_2a_1 + a_2a_3 + a_1a_3 \end{aligned} \quad (2.9.14)$$

which come from $\lambda^3 - \alpha_1\lambda^2 + \alpha_2\lambda - \alpha_3 = (\lambda - a_3)(\lambda - a_2)(\lambda - a_1) = (\lambda - a_1)(\lambda - a_3)(\lambda - a_2) = (\lambda - a_2)(\lambda - a_1)(\lambda - a_3)$. These imply

$$c = [a_2a_1] = [a_1a_3] = [a_3a_2] \neq 0. \quad (2.9.15)$$

Now $[a_1a_2] \neq 0$ implies that $(\lambda - a_1) \nmid_r (\lambda - a_1)(\lambda - a_3)$. It follows as before that

$$a_2 = [a_1a_3]a_1[a_1a_3]^{-1}. \quad (2.9.16)$$

Similarly, we have the remaining formula in (2.9.11). By (2.9.11), $c^3a_ic^{-3} = a_i$, $1 \leq i \leq 3$. Since the a_i generate D it follows that we have (2.9.12). \square

We can now prove

Theorem 2.9.17. *Any central division algebra of degree three is cyclic.*

Proof. We have to prove the existence of a cyclic element not in F . Hence we begin with a non-cyclic element a and apply Lemma 2.9.8 to obtain an element $c \notin F$ such that $c^3 = \gamma 1$, $\gamma \in F$. If this is cyclic we are done. Otherwise, we use this as the element a of the lemma and so we may assume that $a^3 = \alpha 1$, $\alpha \in F$. Then we have $\lambda^3 - \alpha = (\lambda - a_3)(\lambda - a_2)(\lambda - a_1)$ and (2.9.10)-(2.9.12) hold. Now put

$$b_1 = a_1c, b_2 = a_1b_1a_1^{-1} = a_1^2ca_1^{-1}. \quad (2.9.18)$$

Then

$$[b_1b_2] = a_1ca_1^2ca_1^{-1} - a_1^2c^2 = a_1(ca_1^2c - a_1c^2a_1)a_1^{-1}. \quad (2.9.19)$$

Since $a_2a_1a_3 = \alpha = a_3^3$, $a_2a_1 = a_3^2$ and

$$\begin{aligned} 0 &= a_2a_1 - a_3^2 = ca_1c^{-1}a_1 - c^2a_1^2c^{-2} \\ &= c(a_1c^2a_1 - ca_1^2c)/\gamma. \end{aligned}$$

Hence $a_1c^2a_1 = ca_1^2c$ and $[b_1b_2] = 0$. If $b_2 = b_1$ then, by (2.9.18), $c = a_1ca_1^{-1}$ and $a_1c = ca_1$. Since $ca_1c^{-1} = a_2$ this implies $a_2 = a_1$ and $c = 0$ by (2.9.10). Thus $b_2 \neq b_1$. This implies also that $b_1 \notin F$ and since $[b_1b_2] = 0$ and b_2 and b_1 are conjugates it follows from 2.9.7 that b_1 is a cyclic element $\notin F$. \square

The minimum polynomial of b_1 can be calculated to be

$$\lambda^3 + \gamma\lambda - \alpha\gamma. \quad (2.9.20)$$

For, we have

$$\begin{aligned} b_1^2 &= a_1ca_1c = ca_3ca_3 = c^2a_2a_3 \quad (\text{by (2.9.8)}) \\ &= c^2(a_3a_2 - c) = c^2a_3a_2 - \gamma. \end{aligned}$$

Hence

$$b_1^3 + \gamma b_1 = a_1c^3a_3a_2 = \gamma a_1a_3a_2 = \gamma\alpha.$$

$d = 4$. The main structure theorem for central division algebras of degree 4 can be stated in the following way:

Theorem 2.9.21 *Any central division algebra of degree 4 contains a subfield that is a tensor product of two separable quadratic fields.*

This is equivalent to: D is a crossed product (E, G, k) where $G \cong Z_2 \times Z_2$. This result is due to Albert [29]. Quite recently Rowen [78] has given a proof of the theorem that is constructive and is similar to Wedderburn's proof in the degree 3 case.³ We shall give a simplification of Rowen's proof which dispenses with the use of universal division algebras and replaces this by more elementary Zariski topology arguments.

We shall first reduce the proof to showing that D contains a separable quadratic subfield. This reduction is achieved in the following two lemmas.

Lemma 2.9.22 *Let D be a central division algebra over F , a an element of D which is algebraic with minimum polynomial $\lambda^2 - \alpha\lambda - \beta$ where $\alpha \neq 0$. Then there exists an $x \in D$ such that $y = [ax] \neq 0$ and for such an x we have $[ay] = [a[ax]] \neq 0$, $yay^{-1} = \alpha 1 - a$ and $[ay^2] = 0$. Hence $F(y^2) \subsetneq F(y)$.*

Proof. Since $a \notin F1$ there exists an x such that $y = [ax] \neq 0$. We have $a^2 = \alpha a + \beta$. Hence $\alpha[ax] = [a^2x] = a[ax] + [ax]a$. Thus $ay + ya = \alpha y$ and $ya = (\alpha 1 - a)y$. If $[ay] = 0$ then $ay = (a1 - a)y$ so $2a = \alpha 1$. Then $2y = [2a, x] = [\alpha 1, x] = 0$ so $\text{char } F = 2$. But then $\alpha 1 = 2a = 0$ contrary to $\alpha \neq 0$. On the other hand, $y^2a = y(\alpha 1 - a)y = ay^2$. Hence $[ay^2] = 0$. Evidently $[ay] \neq 0$ and $[ay^2] = 0 \Rightarrow F(y^2) \subsetneq F(y)$. Also, $yay^{-1} = \alpha 1 - a$ is clear.

Lemma 2.9.23. *Let D be a central division algebra of degree 4 and let $F(a)$ be a separable quadratic subfield of D . Then there exists a second separable*

³ It should be noted that Rowen's proof is similar to one given by Albert in the characteristic zero case that was published in [32₂].

quadratic subfield $F(b)$ such that the subalgebra $F[a, b]$ generated by a and b is the tensor product $F(a) \otimes_F F(b)$.

Proof. We show first that D contains an element x such that $[ax]^4 \notin F1$. The set of these x 's is an open subset in the Zariski topology. Hence it suffices to show that there is an x in $M_4(\bar{F}) = D_{\bar{F}}$, \bar{F} the algebraic closure of F , such that $[ax]^4 \notin \bar{F}1$. The condition on a implies that if we replace a by a similar matrix we may assume

$$a = \text{diag}\{\alpha_1, \alpha_1, \alpha_2, \alpha_2\}, \alpha_1 \neq \alpha_2. \quad (2.9.24)$$

This follows by elementary linear algebra. For, the minimum polynomial $\mu_a(\lambda)$ is a quadratic polynomial irreducible in $F[\lambda]$ with distinct roots α_1, α_2 in \bar{F} . Then a is similar in $M_4(\bar{F})$ to a diagonal matrix with diagonal entries α_1, α_2 where both α_1 and α_2 occur. Then the characteristic polynomial $\chi_a(\lambda) = \mu_a(\lambda)\nu_a(\lambda)$ where $\nu_a(\lambda) = (\lambda - \alpha_i)(\lambda - \alpha_j)$, $i, j = 1$ or 2 . Since $\chi_a(\lambda) \in F[\lambda]$, $\nu_a(\lambda) \in F[\lambda]$. If $\nu_a(\lambda) = (\lambda - \alpha_i)^2$ then $(\lambda - \alpha_i) = (\mu_a(\lambda), \nu_a(\lambda)) \in F[\lambda]$, contrary to the irreducibility of $\mu_a(\lambda)$ in $F[\lambda]$. Hence $\nu_a(\lambda) = \mu_a(\lambda)$ and (2.9.24) holds. We can write

$$x = \begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix}, \quad X_{ij} \in M_2(\bar{F}). \quad (2.9.25)$$

Then

$$[ax] = \begin{pmatrix} 0 & (\alpha_1 - \alpha_2)X_{12} \\ (\alpha_2 - \alpha_1)X_{21} & 0 \end{pmatrix} = (\alpha_1 - \alpha_2) \begin{pmatrix} 0 & X_{12} \\ -X_{21} & 0 \end{pmatrix}. \quad (2.9.26)$$

Then

$$[ax]^2 = -(\alpha_1 - \alpha_2)^2 \text{diag}\{X_{12}X_{21}, X_{21}X_{12}\} \quad (2.9.27)$$

and if we choose $X_{12} = e_{12}, X_{21} = e_{21}$ we shall have $[ax]^4 \notin \bar{F}1$. This proves the existence of $x \in D$ such that $[ax]^4 \notin F1$.

We shall now show that if $y = [ax]$ and $y^4 \notin F1$ then $b = y^2$ is separable quadratic, $[ab] = 0$ and $F[a, b] = F[a] \otimes_F F[b]$. By 2.9.22, $F[b] \subsetneq F[y]$. Hence $F[b] = F1$ or $[F[b] : F] = 2$. The first case is ruled out since $b^2 \notin F1$. Hence $F[b]$ is quadratic over F and if this is not separable then $b^2 \in F1$ again contradicting $y^4 \notin F1$. Also, by the proof of 2.9.22, $[ab] = [ay^2] = 0$. Finally $[F[a, b] : F] = 4$ since otherwise $a \in F[b]$ and $[ay] = 0$ contrary to the relation $yay^{-1} = \alpha_1 - a$ in 2.9.22.

It remains to show that D contains an element a such that $F(a)$ is separable quadratic. The main step in the proof of this is

Lemma 2.9.28 (Rowen). *Let D be a central division algebra, a_1 an element of D having minimum polynomial $f(\lambda) = \lambda^4 + \alpha_2\lambda^2 - \alpha_3\lambda + \alpha_4$. Then $f(\lambda) = (\lambda^2 - a'\lambda + b')(\lambda^2 - a\lambda + b)$ in $D[\lambda]$ and for any such factorization we have $[F(a^2) : F] < 4$.*

Proof. The existence of the factorization into quadratic factors follows from Wedderburn's factorization theorem (2.9.1). Also we have

$$a' = -a, \quad b' = \alpha_4 b^{-1} \quad (2.9.29)$$

and

$$\alpha_2 = a'a + b + b' = -a^2 + b + \alpha_4 b^{-1} \quad (2.9.30)$$

$$\alpha_3 = a'b + b'a = -ab + \alpha_4 b^{-1}a \quad (2.9.31)$$

We distinguish two cases:

Case I $[ab] = 0$. Then $\alpha_3 = (\alpha_4 b^{-1} - b)a$ and $\alpha_3^2 = [(\alpha_4 b^{-1} + b)^2 - 4\alpha_4]a^2 = [(a^2 + \alpha_2)^2 - 4\alpha_4]a^2 = a^6 + 2\alpha_2 a^4 + (\alpha_2 - 4\alpha_4)a^2$. Thus a^2 is a root of a cubic polynomial so $[F(a^2) : F] < 4$.

Case II $[ab] \neq 0$. By (2.9.31), $[a^2b] = 0$. Since $[ab] \neq 0$ it follows that $F(a^2) \subsetneq F(a)$ so again $[F(a^2) : F] < 4$. \square

To use Rowen's lemma to construct a separable quadratic subfield of D we begin with a pair of elements u, v and form $a_1 = [uv]$. Then the reduced trace $t(a_1) = 0$. Suppose a_1 has degree 4. Then the minimum polynomial $m(\lambda)$ of a_1 over F has the form $m(\lambda) = \lambda^4 + \alpha_2 \lambda^2 - \alpha_3 \lambda + \alpha_4$ and factors in $D[\lambda]$ as $m(\lambda) = (\lambda - a_4)(\lambda - a_3)(\lambda - a_2)(\lambda - a_1) = (\lambda^2 - a'\lambda + b')(\lambda^2 - a\lambda + b)$ where $b = a_2 a_1$, $a = a_1 + a_2$. Also by Theorem 2.9.1, if we choose y so that $[ya_1] = [y[uv]] \neq 0$ then we may assume that $a_2 = [ya_1]a_1[ya_1]^{-1}$. Then

$$a = a_1 + a_2 = a_1 + [ya_1]a_1[ya_1]^{-1} = [y, a_1^2][ya_1]^{-1} \quad (2.9.32)$$

in Rowen's lemma. Now suppose we can choose u, v, y so that $a^4 \notin F$. Then $F(a^2)$ is a separable quadratic subfield since, by Rowen's lemma, $[F(a^2) : F] < 4$ so $[F(a^2) : F] = 2$ or 1 and the latter is ruled out if $a^4 \notin F$. Hence $[F(a^2) : F] = 2$ and $F(a^2)/F$ is separable since otherwise the characteristic is 2 and $(a^2)^2 = a^4 \in F$ contrary to the choice of u, v, y .

We shall now prove

Lemma 2.9.33. *If D is a central division algebra of degree 4 then D contains a separable quadratic subfield.*

Proof. This will follow from the foregoing remarks if we can show that the subset T of $D^{(3)}$ of elements (u, v, y) such that

1. $[u, v]$ is of degree 4
2. $[y, [uv]] \neq 0$
3. $([y, [uv]^2][y, [uv]]^{-1})^4 \notin F$

is not vacuous. We can replace 2. by the polynomial condition

$$2'. \quad n([y, [uv]]) \neq 0$$

n the reduced norm, and 3. can be replaced by

$$3'. \quad ([y, [uv]^2][y, [uv]]^\#)^4 \notin F$$

where $\#$ denotes the reduced adjoint ($x^\# = n(x)x^{-1}$ if x is invertible). Let T_1, T_2, T_3 denote the sets defined by 1, 2', 3' respectively. It is clear that T_1 and T_2 are open in $D^{(3)}$. Since the condition that $x^4 \notin F1$ defines an open subset of D it is clear that T_3 is open. Since the intersection of a finite number of non-vacuous open subsets in the Zariski topology is non-vacuous open, it suffices to show that T_i , $1 \leq i \leq 3$, is non-vacuous and this will be the case if the corresponding subset \bar{T}_i of $M_4(\bar{F})$ is non-vacuous. We proceed to verify this.

The proof of Lemma 2.9.23 shows that we may take

$$[uv] = \begin{pmatrix} 0 & X_{12} \\ X_{21} & 0 \end{pmatrix} \quad (2.9.34)$$

for any $X_{ij} \in M_2(\bar{F})$ and there exist such matrices having minimum polynomials of degree 4 (e.g. $X_{12} = X_{21} = X$ where $X^2 \notin \bar{F}1_2$ and $\det X \neq 0$). Thus $T_1 \neq \emptyset$. We now take $y = \text{diag}\{Y, Y\}$ where $Y \in M_2(\bar{F})$. Then

$$[y[uv]] = \begin{pmatrix} 0 & [YX_{12}] \\ [YX_{21}] & 0 \end{pmatrix} \quad (2.9.35)$$

so evidently $\bar{T}_2 \neq \emptyset$. Also we have $[uv]^2 = \text{diag}\{X_{12}X_{21}, X_{21}X_{12}\}$ so

$$[y, [uv]^2] = \text{diag}\{[Y, X_{12}X_{21}], [Y, X_{21}X_{12}]\}. \quad (2.9.36)$$

For any matrix $Z = \begin{pmatrix} 0 & Z_{12} \\ Z_{21} & 0 \end{pmatrix}$, $Z_{ij} \in M_2(\bar{F})$, we have

$$Z^\# = \begin{pmatrix} 0 & -n(Z_{12})\bar{Z}_{21}^\# \\ -n(Z_{21})\bar{Z}_{12}^\# & 0 \end{pmatrix} \quad (2.9.37)$$

$n(z_{ij}) = \det Z_{ij}$. Hence

$$[y, [uv]]^\# = \begin{pmatrix} 0 & W_{12} \\ W_{21} & 0 \end{pmatrix} \quad (2.9.38)$$

where

$$\begin{aligned} W_{12} &= -n([YX_{12}])[YX_{21}]^\# \\ W_{21} &= -n([YX_{21}])[YX_{12}]^\#. \end{aligned} \quad (2.9.39)$$

By (2.9.35) and (2.9.36)

$$z = [y[uv]^2][y[uv]]^\# = \begin{pmatrix} 0 & Z_{12} \\ Z_{21} & 0 \end{pmatrix} \quad (2.9.40)$$

where

$$Z_{12} = [Y, X_{12}X_{21}]W_{12} \quad Z_{21} = [Y, X_{21}X_{12}]W_{21}. \quad (2.9.41)$$

Hence $z^2 = \text{diag}\{Z_{12}Z_{21}, Z_{21}Z_{12}\}$ and

$$Z_{12}Z_{21} = \delta[Y, X_{12}X_{21}][YX_{21}]^\#[Y, X_{21}X_{12}][YX_{12}]^\# \quad (2.9.42)$$

where $\delta = n([Y X_{12}][Y X_{21}])$.

If we take

$$X_{12} = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, X_{21} = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}, Y = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \quad (2.9.43)$$

a simple calculation shows that

$$\begin{aligned} Z_{12}Z_{21} &= \delta(\alpha - \beta)^4 \text{diag}\{r, s\} \\ r &= c_1c_2(a_1b_2 + c_1d_2)(a_2b_1 + b_2d_1) \\ s &= b_1b_2(c_1a_2 + d_1c_2)(c_2a_1 + d_2c_1). \end{aligned} \quad (2.9.44)$$

It is clear from this formula that the parameters $\alpha, \beta, a_1, \dots$ can be chosen so that $z^4 \notin F1$. Hence $\tilde{T}_3 \neq \emptyset$. This completes the proof. \square

Evidently Lemmas 2.9.23 and 2.9.33 constitute a proof of Theorem 2.9.21.

We shall now apply this theorem to obtain a canonical construction for central division algebras of degree 4 over F . By Theorem 2.9.21, D contains a subfield E/F that is abelian with Galois group $V = \{1, \sigma_1, \sigma_2, \sigma_3\}$ where $\sigma_i^2 = 1, \sigma_i\sigma_j = \sigma_k, i, j, k \neq$. The field E has three quadratic subfields $Q_i, 1 \leq i \leq 3$, where $Q_i = \text{Inv}\langle\sigma_i\rangle$. We have $E = Q_iQ_j \simeq Q_i \otimes_F Q_j$ for $i \neq j$. Let

$$D_i = D^{Q_i}. \quad (2.9.45)$$

Then $[D_i : F] = [D : F]/[Q_i : F] = 8$ and Q_i is the center of D_i . Evidently $D_i \supset E$. The automorphism σ_i of E can be extended to an inner automorphism I_{x_i} of D . Since $\sigma_i \mid Q_i = 1_{Q_i}$ $x_i \in D_i$ and $D_i = E[x_i]$. Then D_i is the cyclic algebra (or quaternion algebra)

$$D_i = (E, \sigma_i, a_i) \quad (2.9.46)$$

over Q_i where $x_i^2 = a_i \in Q_i$. The condition that D_i is a division algebra is that

$$a_i \notin N_{E/Q_i}(b_i) \quad (2.9.47)$$

for $b_i \in E$.

Now let $j \neq i$. Since $I_{x_j}Q_i = Q_i, I_{x_j}D_i = D_i$. It is clear that $D = D_i[x_j] = E[x_i, x_j]$. We shall now make a normalization: We choose $x_3 = x_1x_2$ which can be done since $\sigma_3 = \sigma_1\sigma_2$. Since the restriction of the automorphism $I_{x_2}I_{x_1}I_{x_2^{-1}}$ to E is $\sigma_2\sigma_1\sigma_2^{-1} = \sigma_1$ we have

$$x_2x_1x_2^{-1} = ax_1, \quad a \in E^*. \quad (2.9.48)$$

We have $D = D_1[x_2]$ and if we write $\sigma = I_{x_2} \mid D_1$ then

$$\sigma x_1 = ax_1, \quad \sigma \mid E = \sigma_2 \quad (2.9.49)$$

and $\sigma^2 = I_{a_2}$. Hence it is clear that D is the generalized cyclic algebra $R/R(t^2 - a_2)$, R the twisted polynomial ring $D_1[t; \sigma]$. The condition that this generalized cyclic algebra is a division algebra is that

$$a_2 \neq (\sigma y)y \quad (2.9.50)$$

for $y \in D_1$ (1.3.16).

We now derive some relations connecting the a_i and a . We have $(x_2x_1x_2^{-1})^2 = x_2x_1^2x_2^{-1} = \sigma_2a_1$ and $(ax_1)^2 = ax_1ax_1^{-1}x_1^2 = a(\sigma_1a)a_1$. Hence, by (2.9.48),

$$a(\sigma_1a) = (\sigma_2a_1)a_1^{-1}. \quad (2.9.51)$$

Similarly, since $x_1x_2x_1^{-1} = a^{-1}x_2$ we have

$$a(\sigma_2a) = a_2(\sigma_1a_2)^{-1}. \quad (2.9.52)$$

Also we have $a_3 = x_3^2 = (x_1x_2)^2 = x_1x_2x_1x_2 = x_1ax_1x_2^2 = x_1ax_1^{-1}x_1^2x_2^2 = (\sigma_1a)a_1a_2$. Hence

$$a = (\sigma_1a_3)(a_1(\sigma_1a_2))^{-1} \quad (2.9.53)$$

By (2.9.51) and (2.9.53), we have $(\sigma_2a_1)a_1^{-1} = (\sigma_1a_3)(a_1(\sigma_1a_2))^{-1}a_3(a_1a_2)^{-1} = (\sigma_1a_3)a_1^{-2}a_3(a_2(\sigma_1a_2))^{-1}$ and hence $a_3(\sigma_1a_3) = a_1(\sigma_2a_1)a_2(\sigma_1a_2)$. Thus

$$N_{Q_3/F}(a_3) = N_{Q_1/F}(a_1)N_{Q_2/F}(a_2). \quad (2.9.54)$$

We can now prove

Theorem 2.9.55 (cf. Albert [39], p. 186f). *Let E be a quartic abelian extension of F with Galois group $V = \{1, \sigma_1, \sigma_2, \sigma_3\}$ such that $\sigma_i^2 = 1$, $\sigma_i\sigma_j = \sigma_k$ if $i, j, k \neq$. Then we have the following recipe for constructing the central division algebras of degree four over F containing E :*

1. Let $Q_1 = \text{Inv } \sigma_1$ and choose $a_1 \in E$ such that $a_1 \notin N_{E/Q_1}(E)$. Form the quaternion algebra $D_1 = (E, \sigma_1, a_1)$ over Q_1 . Then D_1 is a division algebra.

2. Let x_1 be a canonical generator of D_1 over E such that $x_1b = (\sigma_1b)x_1, b \in E$. Choose $a \in E$ such that (2.9.51) holds and $a_2 \in E$ such that (2.9.52). Then there is an automorphism σ of D_1/F such that $\sigma x_1 = ax_1$ and $\sigma \mid E = \sigma_2$. Moreover, $\sigma^2 = I_{a_2}$.

3. Let R be the twisted polynomial ring $D_1[t; \sigma_2]$ and $D = R/R(t^2 - a_2)$. Then D is central simple of degree four containing E and D is a division algebra if and only if (2.9.50) holds.

Every central division algebra of degree 4 over F containing E can be obtained in this way.

Proof. 1. This is clear.

2. We have the defining relations

$$x_1b = (\sigma_1b)x_1, \quad b \in E, \quad x_1^2 = a_1 \quad (2.9.56)$$

in D_1 . If we put $x'_1 = ax_1$ then

$$\begin{aligned} x'_1(\sigma_2b) &= (ax_1)(\sigma_2b) = (\sigma_2\sigma_1b)(ax_1) = (\sigma_2\sigma_1b)x'_1 \\ x_1'^2 &= (ax_1)^2 = a(\sigma_1a)x_1^2 = a(\sigma_1a)a_1 = \sigma_2a_1 \end{aligned} \quad (2.9.57)$$

by (2.9.51). Hence we have an automorphism σ of D_1 such that $\sigma x_1 = x'_1$ and $\sigma \mid E = \sigma_1$. Also $\sigma^2 = b, b \in E$, and $\sigma^2 x_1 = \sigma(ax_1) = (\sigma_2 a)ax_1 = a_2(\sigma_1 a_2^{-1})x_1$, by (2.9.52). Hence $\sigma^2 x_1 = I_{a_2} x_1$ so $\sigma^2 = I_{a_2}$.

3. We can form the generalized cyclic algebra $D = R/kR(t^2 - a_2)$ where $R = D_1[t; \sigma]$. This is central simple of degree 4 (see section 1.4). By Theorem 1.3.16, D is a division algebra if and only if (2.9.51) holds.

The fact that every central division algebra of degree 4 containing E is obtained following this procedure is clear from the analysis preceding 2.9.55. \square

2.10. Non-cyclic Division Algebras of Degree Four

Albert has given a number of constructions of non-cyclic division algebras of degree four. His first construction was that of a tensor product of quaternion algebras. Later he gave two other constructions which are not tensor products of quaternion algebras, one containing an element a with minimum polynomial of the form $\lambda^4 - \alpha$ and one containing no such element ([32], [33], [38]). All of the constructions are based on a result on cyclic quartic fields that we shall derive. For this we shall need the following norm theorem.

Lemma 2.10.1 (Albert [39]). *Let E/F be cyclic with Galois group $G = \langle \sigma \rangle$ of order $r = r_1 r_2$. Suppose γ is an element of F^* such that $\gamma^{r_1} = N_{E/F}(c)$, $c \in E$. Then there exists a $c_1 \in E_1 = \text{Inv}\langle \sigma^{r_2} \rangle$ such that $\gamma = N_{E_1/F}(c_1)$.*

This can be proved quite easily using commutative methods. However, we prefer to give a non-commutative proof of a more general result which we state as

Lemma 2.10.1'. *Let D be a division ring with an automorphism σ such that $\sigma^r = 1$ and r is the order of σ modulo inner automorphisms. Suppose $r = r_1 r_2$ and γ is a non-zero element of $F = \text{cent } D \cap \text{Inv}\langle \sigma \rangle$ such that there exists a c satisfying $\gamma^{r_1} = N_r(c) = (\sigma^{r-1}c)(\sigma^{r-2}c) \cdots c$. Then there exists a $c_1 \in \text{Inv}\langle \sigma^{r_2} \rangle$ such that $\gamma = N_{r_2}(c) = (\sigma^{r_2-1}c_1)(\sigma^{r_2-2}c_1) \cdots c_1$.*

Proof. Let R be the twisted polynomial ring $D[t; \sigma]$. By Theorem 1.1.23, $\text{Cent } R = F[t^r]$. Then $t^r - \gamma^{r_1}$ is a two-sided irreducible element of R and $(t^{r_2} - \gamma) \mid (t^r - \gamma^{r_1})$. Since $\gamma^{r_1} = N_r(c)$, $(t - c) \mid (t^r - \gamma^{r_1})$ (1.3.11). By Corollary 1.3.15, $t^r - \gamma^{r_1}$ is a product of factors of degree 1. Hence the same is true of the factor $t^{r_2} - \gamma$ of $t^r - \gamma^{r_1}$. Then $\gamma = N_{r_2}(c_1) = (\sigma^{r_2-1}c_1)(\sigma^{r_2-2}c_1) \cdots c_1$ for some $c_1 \in D$. Since $\sigma\gamma = \gamma$ we also have $\gamma = (\sigma^{r_2}c_1)(\sigma^{r_2-1}c_1) \cdots (\sigma c_1) = (\sigma^{r_2-1}c_1) \cdots (\sigma c_1)(\sigma^{r_2}c_1)$. Hence $\sigma^{r_2}c_1 = c_1 \in \text{Inv}\langle \sigma^{r_2} \rangle$. \square

We can now prove the following

Lemma 2.10.2. *Let F be a field not containing $\sqrt{-1}$ (so $\text{char } F \neq 2$) and let E be a cyclic quartic extension field of F then the (unique) quadratic subfield K of E/F has the form $F(\sqrt{u^2 + v^2})$ where $u, v \in F$ and $u^2 + v^2$ is not the square of an element of F .*

Proof. Since $\text{char } F \neq 2$, $K = F(\sqrt{w})$, w not a square in F . Now $1 = (-1)^2 = N_{E/F}(1)$. Hence by 2.10.1, $-1 = N_{K/F}(c_1)$, $c_1 \in K$. We have $c_1 = a + b\sqrt{w}$, $a, b \in F$. Then

$$-1 = N_{K/F}(c_1) = (a + b\sqrt{w})(a - b\sqrt{w}) = a^2 - b^2w.$$

Now $b \neq 0$ since $\sqrt{-1} \notin F$. Hence $b^2w = a^2 + 1$ gives $w = u^2 + v^2$, $u = ab^{-1}$, $v = b^{-1}$. \square

Lemma 2.10.2 suggests a procedure for constructing a non-cyclic division algebra of degree four: It suffices to construct a division algebra of degree 4 such that $D \otimes_F K$ is a division algebra for every quadratic extension field $K = F(\sqrt{u^2 + v^2})$, $u, v \in F$. For, then D contains no quadratic subfield of the form $F(\sqrt{u^2 + v^2})$ and hence, by 2.10.2, D contains no cyclic quartic subfield.

We shall need a condition that the tensor product of two quaternion division algebras is a division algebra. A first such condition is given in

Theorem 2.10.3 (Albert [72], Sah [72]). *Let D_i , $i = 1, 2$, be a quaternion division algebra over the field F . Then $D_1 \otimes_F D_2$ is not a division algebra if and only if D_1 and D_2 contain isomorphic quadratic subfields.*

Proof. The condition is sufficient since the tensor product of isomorphic finite dimensional extension fields $\neq F$ is never a field. Now suppose $D_1 \otimes_F D_2$ is not a division algebra. We regard D_1 and D_2 as subalgebras of $D_1 \otimes_F D_2$ such that D_1 centralizes D_2 . Let Q be a separable quadratic subfield of D_2 and let σ be the automorphism $\neq 1$ of Q/F . We have $Q = F(u)$ where $u^2 = u + \alpha$, $\alpha \in F$, and $\sigma u = 1 - u$. There exists a $v \in D_2$ such that

$$vu = (1 - u)v, \quad v^2 = \beta \in F. \quad (2.10.4)$$

Suppose $QD_1 = Q \otimes_F D_1$ is not a division algebra. Then Q is a splitting field for D_1 and hence Q is isomorphic to a subfield of D_1 and D_1 and D_2 have isomorphic quadratic subfields. Now suppose QD_1 is a division algebra. Then it is readily seen that $D_1D_2 = D_1 \otimes_F D_2 = QD_1[v]$ is a generalized cyclic algebra $R/R(t^2 - \beta)$ where $R = QD_1[t; \sigma]$ and $\sigma \mid D_1 = 1_D$, $\sigma u = 1 - u$. Since D_1D_2 is not a division algebra there exists a $d \in QD_1$ such that $(\sigma d)d = \beta$ (Theorem 1.3.16). We have $d = d_1 + ud_2$, $d_i \in D_1$, $\sigma d = d_1 + (1 - u)d_2$ and the conditions $\beta = (\sigma d)d$, $u^2 = u + \alpha$ imply $d_1d_2 = d_2d_1$ so $Q' = F(d_1, d_2)$ is a subfield of D_1 . Now consider $Q'D_2$. This contains $Q'Q \cong Q' \otimes_F Q$. If this is not a field then $Q' \cong Q$ and the result holds in this case. Now suppose $Q'Q$ is a field. Then $Q'D_2$ is the cyclic algebra $(Q'Q, \sigma', \beta)$ where $\sigma' \mid Q' = 1_{Q'}$, $\sigma'u = 1 - u$. We have $\beta = (\sigma'd)d$ for $d = d_1 + ud_2 \in Q'Q$. Hence $Q'D_2 \sim 1$

and Q' is a splitting field for D_2 . Then $[Q' : F] = 2$ and Q' is isomorphic to a subfield of D_2 . Since $Q' \subset D_1$ this proves the result in this case. \square

We now assume $\text{char } F \neq 2$ and we shall obtain a quadratic form condition that the tensor product of two quaternion algebras over F is a division algebra. A quaternion algebra D_i has a base $(1, u_i, v_i, u_i v_i)$ over F such that

$$u_i^2 = \alpha_i, v_i^2 = \beta_i, u_i v_i = -v_i u_i \quad (2.10.5)$$

where $\alpha_i \beta_i \neq 0$. If both α_i and β_i are squares then we may take these to be 1 and it is readily seen that $D_i \cong M_2(F)$. If α_i (or β_i) is a non-square then clearly D_i is a cyclic algebra. In any case D_i is central simple of degree 2. Let t_i and n_i be the reduced trace and norm respectively on D_i . If $x_i = \xi_0 + \xi_1 u_i + \xi_2 v_i + \xi_3 u_i v_i$ then we have $t(x_i) = 2\xi_0$ and

$$n(x_i) = \xi_0^2 - \alpha_i \xi_1^2 - \beta_i \xi_2^2 + \alpha_i \beta_i \xi_3^2. \quad (2.10.6)$$

The subspace $D'_i = Fu_i + Fv_i + Fu_i v_i$ is the set of elements of trace 0. On this subspace (2.10.6) reduces to

$$n(x_i) = -\alpha_i \xi_1^2 - \beta_i \xi_2^2 + \alpha_i \beta_i \xi_3^2. \quad (2.10.7)$$

D_i is a division algebra if and only if n_i is anisotropic on D'_i . For, D_i is central simple and hence D_i is not a division algebra if and only if it contains an element $x_i \neq 0$ such that $x_i^2 = 0$. For such an x_i we have $t_i(x_i) = 0 = n(x_i)$ so n_i is not anisotropic on D'_i . Conversely, if n_i is not anisotropic on D'_i then we have an $x_i \neq 0$ with $t(x_i) = 0 = n(x_i)$. Then $x_i^2 = 0$.

We now form $D'_1 \oplus D'_2$ and define a quadratic form on this vector space by

$$n(x_1 + x_2) = n_1(x_1) - n_2(x_2), \quad x_i \in D'_i. \quad (2.10.8)$$

Then we have the following result which is also due to Albert [32₁].

Theorem 2.10.9. *Let D_i , $i = 1, 2$, be a quaternion algebra over a field F of characteristic $\neq 2$, D'_i the subspace of D_i of elements of reduced trace 0, n_i the reduced norm on D_i . Define the quadratic form n on $D'_1 \oplus D'_2$ by (2.10.8). Then $D_1 \otimes_F D_2$ is a division algebra if and only if n is anisotropic.*

Proof. If either D_1 or D_2 is not a division algebra then neither is $D_1 \otimes_F D_2$. Moreover, since n_i is not anisotropic on D'_i for $i = 1$ or 2 it is clear that n is not anisotropic on $D'_1 \oplus D'_2$. Now assume D_1 and D_2 are division algebras and $D_1 \otimes_F D_2$ is not. Then, by 2.10.3, D_i contains a quadratic subfield Q_i with $Q_1 \cong Q_2$. Now $Q_i = F(x_i)$ where $x_i^2 + n_i(x_i)1 = 0$. Since $Q_1 \cong Q_2$ we may suppose $n_1(x_1) = n_2(x_2)$. Then $n(x_1 + x_2) = 0$ and n is not anisotropic. Conversely, suppose we have $x_i \in D'_i$ such that $x_1 + x_2 \neq 0$ and $n(x_1 + x_2) = 0$. Since D_i is a division algebra, $x_i \neq 0 \Rightarrow n_i(x_i) \neq 0$. Hence $x_1 \neq 0$, $x_2 \neq 0$ and $n_1(x_1) = n_2(x_2)$. It follows that if we put $Q_i = F(x_i)$ then Q_1 and Q_2 are isomorphic quadratic fields and hence $D_1 \otimes_F D_2$ is not a division algebra by Theorem 2.10.3. \square

We are now ready to define Albert's first class of examples of non-cyclic division algebras of degree 4. Let F_0 be a real field (= subfield of \mathbf{R}) and let $F = F_0(\xi, \eta)$, ξ, η indeterminates. Put $S = F_0[\xi, \eta]$. We order the monomials $\xi^i \eta^j$ lexicographically and if $f(\xi, \eta) \in S$ and $f(\xi, \eta) \neq 0$ then we define the *leading coefficient* to be the coefficient of the highest monomial (in the lexicographic ordering) occurring in $f(\xi, \eta)$ and $f(\xi, \eta)$ is called *monic* if its leading coefficient is 1. If the highest monomial occurring in $f(\xi, \eta)$ is $\xi^i \eta^j$ then we call $((-1)^i, (-1)^j)$ the *signature*, $\text{sig} f(\xi, \eta)$ of $f(\xi, \eta)$.

Let D_i be the quaternion algebra over F with base $(1, u_i, v_i, u_i v_i)$ such that (2.10.5) holds where $\alpha_1 = \eta$, $\alpha_2 = \xi$, the $\beta_i \neq 0 \in S$, are monic and $\text{sig } \beta_1 = (1, -1)$, $\text{sig } \beta_2 = (-1, -1)$. For example, we may take $\beta_1 = \eta$, $\beta_2 = \xi\eta$. We have

Theorem 2.10.10. $D = D_1 \otimes_F D_2$ is a non-cyclic division algebra.

Proof. This will follow if we can show that for any quadratic extension field $K = F(\gamma)$, $\gamma = \sqrt{\alpha^2 + \beta^2}$, $\alpha, \beta \in F$, D_K is a division algebra. Observe that such quadratic extension fields exist. For example, $\xi^2 + 1$ is not a square in F and hence we can take $\gamma = \sqrt{\xi^2 + 1}$. Now D_K a division algebra implies D a division algebra and if D_K is a division algebra for every quadratic extension $K = F(\sqrt{\alpha^2 + \beta^2})$ then D contains no quadratic subfield of the form $F(\sqrt{\alpha^2 + \beta^2})$ and hence, by Lemma 2.10.2, D contains no cyclic quartic subfield. Since we can replace $\gamma = \sqrt{\alpha^2 + \beta^2}$ by $\mu\gamma$, $\mu \neq 0$ in F and $\mu\gamma = \sqrt{\mu^2(\alpha^2 + \beta^2)}$ it suffices to prove the result for $\gamma = \sqrt{\alpha^2 + \beta^2}$ with $\alpha, \beta \in S$. Since $(D_1 \otimes_F D_2)_K \cong D_{1K} \otimes_K D_{2K}$ it suffices to show that $D_{1K} \otimes_K D_{2K}$ is a division algebra. This will follow from Theorem 2.10.9 if we can show that

$$-n(\xi_1, \dots, \xi_6) = (\eta\xi_1^2 + \beta_1\xi_2^2 - \eta\beta_1\xi_3^2) - (\xi\xi_4^2 + \beta_2\xi_5^2 - \xi\beta_2\xi_6^2) \quad (2.10.11)$$

$= 0$ for $\xi_i \in K$ only if every $\xi_i = 0$. We can write

$$\xi_i = \mu_i + \nu_i\gamma, \quad \mu_i, \nu_i \in F \quad (2.10.12)$$

and it suffices to prove the assertion for $\mu_i, \nu_i \in S$. We have

$$\xi_i^2 = (\mu_i^2 + \nu_i^2\gamma^2) + 2\mu_i\nu_i\gamma \quad (2.10.13)$$

and since $(1, \gamma)$ is a base for K/F , $n(\xi_1, \dots, \xi_6) = 0$ implies that

$$\eta\lambda_1 + \beta_1\lambda_2 - \eta\beta_1\lambda_3 - \xi\lambda_4 - \beta_2\lambda_5 + \xi\beta_2\lambda_6 = 0 \quad (2.10.14)$$

for

$$\lambda_i = \mu_i^2 + \nu_i^2\gamma^2 = \mu_i^2 + \nu_i^2(\alpha^2 + \beta^2). \quad (2.10.15)$$

Moreover, if $\xi_i \neq 0$ then either μ_i or $\nu_i \neq 0$ and hence $\lambda_i = \mu_i^2 + \nu_i^2\gamma^2 \neq 0$ since F_0 is real. Thus it suffices to show that (2.10.14) holds with the λ_i as in (2.10.15) only if every $\lambda_i = 0$. Since F_0 is real a sum of squares of elements

of S is either 0 or it has signature $(1, 1)$ and positive leading coefficient. It follows from the choice of β_1 and β_2 that we have the following table:

$$\begin{aligned}\eta\lambda_1 &= 0 \text{ or sig } \eta\lambda_1 = (1, -1) \\ \beta_1\lambda_2 &= 0 \text{ or sig } \beta_1\lambda_2 = (1, -1) \\ \eta\beta_1\lambda_3 &= 0 \text{ or sig } \eta\beta_1\lambda_3 = (1, 1) \\ \xi\lambda_4 &= 0 \text{ or sig } \xi\lambda_4 = (-1, 1) \\ \beta_2\lambda_5 &= 0 \text{ or sig } \beta_2\lambda_5 = (-1, -1) \\ \xi\beta_2\lambda_6 &= 0 \text{ or sig } \xi\beta_2\lambda_6 = (1, -1).\end{aligned}$$

In all the cases in which we have $\neq 0$ the leading coefficient is positive. Now suppose some λ_i for which (2.10.14) holds is $\neq 0$. Let $\xi^i\eta^k$ be the highest monomial occurring among the terms listed above. We cannot have $((-1)^j, (-1)^k) = (1, 1), (-1, 1)$ or $(-1, -1)$ since the table shows that in these cases $\xi^j\eta^k$ occurs only in a single term in the list contrary to (2.10.14). Thus the only possibility is $((-1)^i, (-1)^k) = (1, -1)$ and $\xi^i\eta^k$ occurs only in $\eta\lambda_1, \beta_1\lambda_2$ and $\xi\beta_2\lambda_6$. Since all of these terms have coefficients 1 in the left hand side of (2.10.14) this equation holds only if every $\lambda_i = 0$. \square

2.11. A Criterion for Cyclicity of a Division Algebra of Prime Degree

It is an open question whether or not all central division algebras of prime degree are crossed products, or, equivalently, are cyclic algebras. For $p = 2$ and 3 this was proved in Section 2.9. For $p \geq 5$ the question is open. If $D = (E, \sigma, \gamma)$ is of prime degree p then D contains an element $u \notin F$ such that $u^p \in F$. We shall now prove that this necessary condition that a central division algebra of prime degree is cyclic is also sufficient. In fact, we shall prove a somewhat stronger result that given u such that $u \notin F, u^p \in F$, then there exists a cyclic subfield E/F of D/F of degree p such that $uEu^{-1} = E$ and $\sigma = I_u \mid E$ is a generator of the automorphism group of E . Then $D = (E, \sigma, \gamma)$ and u can be taken to be the canonical generator of D relative to $E : ua = (\sigma a)u, u^p = \gamma$.

We dispose first of the easy case in which $\text{char } F = p$. Suppose D is a central division algebra of degree p and characteristic p and D contains an element $u \notin F$ such that $u^p \in F$. Consider the derivation $i_u : x \rightsquigarrow [ux]$. We have $i_u \neq 0$ and $i_u^p = i_{u^p} = 0$. Hence there exists a v in D such that $i_uv \neq 0$ but $i_u^2v = 0$. Put

$$w = u(i_uv)^{-1}v. \quad (2.11.1)$$

Then since u and i_uv are i_u -constants, $i_uw = u$. Thus $uw - wu = u$ and

$$uww^{-1} = w + 1. \quad (2.11.2)$$

Put $E = F(w)$. Then (2.11.2) implies that $uEu^{-1} = E$. Since $[E : F] = p$ it follows that E/F is cyclic with $\sigma = I_u \mid E$ as generator of $\text{Gal } E/F$.

We now assume $\text{char } F \neq p$ and we proceed to derive some results on cyclic fields of degree p that we shall require. Let $W = F(\xi)$ where ξ is a primitive p -th root of unity. Then it is an elementary result of Galois theory that W/F is cyclic and $[W : F] = s \mid p - 1$. Hence $\text{Gal } W/F = \langle \tau \rangle$ where $\tau(\xi) = \xi^t$, $0 < t < p$, and s is the order of $t + (p)$ in $(\mathbb{Z}/(p))^*$. We now consider an extension K/W of the form $W(\sqrt[p]{a})$, $a \in W$, and we prove the following sufficient condition that K is cyclic over F .

Lemma 2.11.3. *Let $W = F(\xi)$ where ξ is a primitive p -th root of 1 and let τ be a generator of $\text{Gal } W/F$ and $\tau(\xi) = \xi^t$. Let a be an element of W that is not a p -th power and $(\tau a)a^{-t}$ is a p -th power in W . Then $K = W(\sqrt[p]{a})$ is cyclic over F of degree ps where $s \mid p - 1$ and $K = W \otimes_F E$ where E is the unique subfield of degree p of K/F .*

Proof. Put $r = \sqrt[p]{a}$. Since a is not a p -th power, $[K : W] = p$ and we have the automorphism σ of K/W such that $\sigma(r) = \xi r$. Then σ has order p . We have $\tau(a) = b^p a^t$ for $b \in W$ so $\tau(a) = (br^t)^p$. It follows that the automorphism τ of W/F can be extended to an automorphism τ of K/F such that $\tau(r) = br^t$. Since $\sigma \mid W = 1_W$ and

$$\sigma\tau(r) = b\xi^t r^t, \quad \tau\sigma(r) = \tau(\xi r) = \xi^t br^t \quad (2.11.4)$$

σ and τ are commuting elements of $\text{Gal } K/F$. Since σ has order p and τ has order a multiple of s (the order of $\tau \mid W$), $\langle \sigma, \tau \rangle$ contains an element η of order sp . Since $[K : F] = [K : W][W : F] = ps$ it follows that $\text{Gal } K/F = \langle \eta \rangle$. Hence K is cyclic of degree ps over F and hence K contains a unique cyclic subfield E/F of degree p . Evidently $K = W \otimes_F E$. \square

Let s and t be as above. Then $(s, p) = 1 = (t, p)$ so we have integers s', t' such that $ss' \equiv 1 \pmod{p}$ and $tt' \equiv 1 \pmod{p}$. Now put

$$t_k = s' t'^k = t_{k-1} t', \quad 0 \leq k \leq s. \quad (2.11.5)$$

Then

$$\sum_1^s t^k t_k = s' \left(\sum_1^s (tt')^k \right) \equiv 1 \pmod{p} \quad (2.11.6)$$

and since $t^s \equiv 1 \pmod{p}$, $t'^s \equiv 1 \pmod{p}$ and

$$t_s = s' t'^s \equiv s' \pmod{p}. \quad (2.11.7)$$

The following lemma gives a construction of elements $a \in W$ satisfying the second condition: $(\tau a)a^{-t}$ is a p -th power in W , of Lemma 2.11.3.

Lemma 2.11.8. *Let $a \in W^*$ and put*

$$M(a) = \prod_1^s (\tau^k a)^{t_k}. \quad (2.11.9)$$

Then $(\tau M(a))M(a)^{-1}$ is a p -th power in W .

Proof. Let W^{*p} be the subgroup of W^* of p -th powers. If $a, b \in W^*$ we write $a =_p b$ if $aW^{*p} = bW^{*p}$. We have

$$\tau M(a) = \prod_1^s (\tau^{k+1} a)^{t_k} = (\tau^{s+1} a)^{t_s} \prod_2^s (\tau^k a)^{t_{k-1}}.$$

Since $\tau^{s+1} = \tau$ and $t_s \equiv s' = t_0 \pmod{p}$ we have

$$\tau M(a) =_p \prod_1^s (\tau^k a)^{t_{k-1}}. \quad (2.11.10)$$

On the other hand,

$$M(a)^t = \prod_1^s (\tau^k a)^{tt_k} = \prod_1^s (\tau^k a)^{tt't_{k-1}}$$

and since $tt' \equiv 1 \pmod{p}$

$$M(a)^t =_p \prod_1^s (\tau^k a)^{t_{k-1}}. \quad (2.11.11)$$

Comparison of (2.11.10) and (2.11.11) shows that $(\tau M(a))M(a)^{-t} \in W^{*p}$. \square

We can now prove

Theorem 2.11.12. *Let D be a central division algebra of prime degree over F containing an element $u \notin F$ such that $u^p \in F$. Then there exists a cyclic subfield E of D of prime degree over F such that $uEu^{-1} = E$ and $\sigma = I_u \mid E$ is a generator of $\text{Gal } E/F$.*

Proof (cf. Albert [38₂]). The result has been proved if $\text{char } F = p$. Hence assume $\text{char } F \neq p$. As above, let $W = F(\xi)$, ξ a primitive p -th root of 1. Then $p \nmid [W : F]$ and D_W is a division algebra. Now D_W contains the subfield $K = F(u) \otimes_F W = W(u)$. If $u^p = \gamma \in F$ then K is the splitting field over F of $\lambda^p - \gamma$. We have the automorphism σ of K/W such that $\sigma(u) = \xi u$. Then $\text{Gal } K/W = \langle \sigma \rangle$ and this is a normal subgroup of $\text{Gal } K/F$. Since K/W is cyclic with σ as generator of the Galois group we have

$$D_W = (K, \sigma, \delta), \quad \delta \in W \quad (2.11.13)$$

as algebra over W . Then we have an element $v \in D_W$ such that

$$va = (\sigma a)v, \quad a \in K, \quad v^p = \delta \in W. \quad (2.11.14)$$

We know also that W/F is cyclic with $\text{Gal } W/F = \langle \tau \rangle$ where $\tau(\xi) = \xi^t$ and $[W : F] = s$ where s is the order of $t + (p)$ in $(\mathbf{Z}/(p))^*$. The automorphism τ has a unique extension to an automorphism τ of $D_W = W \otimes_F D$ which is the identity on D . As a special case of (2.11.14) we have

$$vu = \xi uv. \quad (2.11.15)$$

Applying τ to this we obtain, since $\tau(u) = u$,

$$\tau(v)u = \xi^t u \tau(v). \quad (2.11.16)$$

Since $v^t u = \xi^t u v^t$ we obtain

$$\tau(v) = v^t a_1, \quad a_1 \in K. \quad (2.11.17)$$

Then $\tau(\delta) = \tau(v^p) = (a_1 v^t)^p \sigma^p(\sigma^t a_1)(\sigma^{2t} a_1) \cdots (\sigma^{(p)t} a_1) v^{tp}$. Since $(p, t) = 1$, $\text{Gal } K/W = \langle \sigma^t \rangle$ and hence we have

$$\tau(\delta) = N_{K/W}(a_1) \delta^t. \quad (2.11.18)$$

If we apply τ to this and note that $\tau \in \text{Gal } K/F$ and $\langle \sigma \rangle \triangleleft \text{Gal } K/F$ we obtain $\tau^2(\delta) = N_{K/W}(a_2) \delta^{t^2}$. Iteration of this gives

$$\tau^k(\delta) = N_{K/W}(a_k) \delta^{t^k}, \quad a_k \in K. \quad (2.11.19)$$

Now define t_k as in (2.11.5). Then, by (2.11.19),

$$M(\delta) = \prod_1^s (\tau^k \delta)^{t_k} = N_{K/W}(a) \delta^{\sum t_k t^k}, \quad a \in K. \quad (2.11.20)$$

Since, by (2.11.6), $\sum t_k t^k \equiv 1 \pmod{p}$ and $[K : W] = p$ we see that δ and $M(\delta)$ differ by the norm of an element of K . It follows that we can replace v by an element $w = bv, b \in K$, and obtain $wa = (\sigma a)w, a \in K, w^p = M(\delta)$. By Lemma 2.11.8, $M(\delta) \in W$ has the property that $(\tau M(\delta))M(\delta)^{-t}$ is a p -th power in W . Moreover, since $D_W \not\sim 1$, $M(\delta)$ is not a p -th power in W . Hence, by Lemma 2.11.3, $W(w)$ contains a unique cyclic subfield E/F of degree p . Since $w = bv, b \in K$, we have from (2.11.15), that

$$u^{-1}wu = \xi w. \quad (2.11.21)$$

Since $W(w)/F$ is cyclic of degree sp and $[W : F] = s$ we have $W(w) = W \otimes_F E$. Since $I_u \mid W = 1_W$ it follows from (2.11.21) that $u^{-1}W(w)u = W(w)$ and since E is the only subfield of degree p of $W(w)$ we see that $I_u \mid E$ is an automorphism ρ of E/F such that $\text{Gal } E/F = \langle \rho \rangle$. It follows that E and u generate an F -subalgebra of D_W that is a cyclic algebra (E, ρ, γ) . Then $D_W = W \otimes_F D = W \otimes_F (E, \rho, \gamma)$. Then

$$W \otimes_F D \otimes_F (E, \rho, \gamma^{-1}) \sim 1 \text{ in } \text{Br}(W).$$

Since the degree of $D \otimes_F (E, \rho, \gamma^{-1})$ is p^2 and $[W : F] = s$ it follows that $D \otimes_F (E, \rho, \gamma^{-1}) \sim 1$ in $\text{Br}(F)$. Then $D \cong (E, \rho, \gamma)$. This isomorphism implies that we have an element $u' \in D$ such that $u'^p = \gamma$ and a cyclic subfield E' such that $I_{u'} \mid E'$ is an automorphism generating $\text{Gal } E'/F$. Then $F(u') \cong F(u)$ under an automorphism such that $u' \rightsquigarrow u$. This isomorphism can be extended

to an inner automorphism of D . The image of E' under this automorphism is a field E/F satisfying the conditions of the theorem. \square

2.12. Central Division Algebras of Degree Five

We shall now apply the cyclicity result of the last section to derive a result of Brauer's ([38]) on splitting fields of central division algebras of degree five.

Let D be a central division algebra of degree n over F , $K = F(u)$ a maximal separable subfield of D , $f(\lambda)$ the minimum polynomial of u , $E = F(r_1, \dots, r_n)$ a splitting field of $f(\lambda)$ where $f(\lambda) = \Pi(\lambda - r_i)$. As we have seen in Theorem 2.3.17 and its proof, we can identify D with the F -subalgebra of $M_n(E)$ of matrices of the form $(\ell_{ij}c_{ij})$ where $v = (c_{ij})$ is fixed with every $c_{ij} \neq 0$ and $\ell = (\ell_{ij})$ satisfies the conjugacy conditions (2.3.5). Since $D_E = M_n(E)$ the characteristic polynomial of the matrix $(\ell_{ij}c_{ij}) \in D$ is the reduced characteristic polynomial of this element of D and hence its coefficients are contained in F . This polynomial is

$$\chi(\lambda) = \det[\lambda I - (\ell_{ij}c_{ij})] = \lambda^n - h_1\lambda^{n-1} + \dots + (-1)^n h_n \quad (2.12.1)$$

where h_k is the sum of the principal minors of rank k of $(\ell_{ij}c_{ij})$. Now let $g(\lambda) = a_0 + a_1\lambda + \dots + a_{n-1}\lambda^{n-1} \neq 0$ for $a_i \in F$ and define ℓ_{ij} by

$$\ell_{ii} = 0, \ell_{ij} = g(r_i)^{-1} \text{ for } i \neq j. \quad (2.12.2)$$

Then these satisfy the conjugacy conditions and $(\ell_{ij}c_{ij}) \in D$. We shall now derive a set of conditions on the a_i to insure that $h_1 = \dots = h_{n-1} = 0$ and hence that the reduced characteristic polynomial of the element $(\ell_{ij}c_{ij})$ reduces to $\lambda^n + (-1)^n h_n$.

For this purpose we introduce n indeterminates ξ_i . Then $\tilde{D} = D_{F(\xi_1, \dots, \xi_n)}$ over $\tilde{F} = F(\xi_1, \dots, \xi_n)$ is a central division algebra and $\tilde{K} = \tilde{F}(u)$ is a maximal subfield of \tilde{D} (Proposition 1.9.1). We have the splitting field $\tilde{E} = \tilde{F}(r_1, \dots, r_n)$ of $f(\lambda)$. We can regard \tilde{D} as the set of matrices $(\tilde{\ell}_{ij}c_{ij})$ where the $\tilde{\ell}_{ij} \in \tilde{E}$ satisfy the conjugacy conditions. The characteristic polynomial $\tilde{\chi}$ of such a matrix has coefficients in \tilde{F} . Now choose $\tilde{\ell}_{ii} = 0, \tilde{\ell}_{ij}\tilde{g}(r_i)^{-1} = (\xi_0 + \xi_1 r_i + \dots + \xi_{n-1} r_i^{n-1})^{-1}$ for $i \neq j$. This gives an element of \tilde{D} whose characteristic polynomial is $\tilde{\chi}(\lambda) = \lambda^n - \tilde{h}_1\lambda^{n-1} + \dots + (-1)^n \tilde{h}_n$. Since \tilde{h}_k is the sum of the principal minors of rank k of $(\tilde{\ell}_{ij}c_{ij})$ it is clear that if we put

$$P_{n-k} = \tilde{h}_k \prod_{i=1}^n \tilde{g}(r_i) \quad (2.12.3)$$

Then $P_{n-k} = P_{n-k}(\xi_0, \dots, \xi_{n-1})$ is a homogeneous polynomial of degree $n-k$ in the ξ 's. Since \tilde{h}_k and $\Pi \tilde{g}(r_i) \in \tilde{F}$ the coefficients of $P_{n-k}(\xi_0, \dots, \xi_{n-1})$ are contained in F . Also since $\tilde{\ell}_{ii} = 0, h_1 = 0$ and hence $P_{n-1}(\xi_0, \dots, \xi_{n-1}) = 0$. It is clear that if the $a_k \in F$ satisfy

$$P_{n-k}(a_0, \dots, a_{n-1}) = 0, \quad 2 \leq k \leq n-1 \quad (2.12.4)$$

and $(a_1, \dots, a_{n-1}) \neq 0 = (0, \dots, 0)$ then the corresponding element of D satisfies a pure equation $\lambda^n + (-1)^n h_n = 0$. Moreover, since the $\ell_{ii} = 0$ it is clear that the element is not in F . If n is a prime it will follow from Theorem 2.11.2 that D is cyclic.

Now let $n = 5$ and, for the sake of simplicity, assume $\text{char } F \neq 2$. In this case we have the three conditions $P_3(a_0, \dots, a_4) = P_2(a_0, \dots, a_4) = P_1(a_0, \dots, a_4) = 0$ where $P_k(\xi_0, \dots, \xi_4)$ is a homogeneous polynomial of degree k . Now $P_1 = 0$ defines a hyperplane. Hence the determination of the a_i satisfying $P_3 = P_2 = P_1 = 0$ amounts to determining a point of intersection of a quadric and a cubic surface in projective four space. While such an intersection may not exist for the base field F we claim that it does exist in an extension field obtained by adjoining two square roots of elements of F and then the root of a cubic equation. To see this we note that we may assume the quadric is given by $P_2 = \sum_1^4 \alpha_1 x_i^2$. Then it is readily seen that if we adjoin $\sqrt{-\alpha_1 \alpha_2}, \sqrt{-\alpha_3 \alpha_4}$ to F we obtain a line on P_2 . To obtain a point of intersection of P_2 with the cubic surface $P_3 = 0$ it suffices to obtain an intersection of this line with $P_3 = 0$. This can be done if the field is extended by a root of a cubic equation. We therefore have the following

Theorem 2.12.5 (Brauer [38]). *Let D be a central division algebra of degree five over F ($\text{char } F \neq 2$). Then there exists a field K of the form $F(\sqrt{\alpha}, \sqrt{\beta}, \theta)$ where $\alpha, \beta \in F$ and θ is a root of a cubic equation over $F(\sqrt{\alpha}, \sqrt{\beta})$ such that D_K is cyclic.*

This shows also that D has a splitting field E such that E contains a subfield K over which E is cyclic of degree five and K is as in the theorem. If $\text{char } F \neq 2, 3$ then the normal closure of E is solvable, that is, is Galois with solvable Galois group. Hence we have

Corollary 2.12.6. *Any central division algebra of degree five has a solvable splitting field.*

Note. Rosset has shown in [77] that if F contains p distinct p -th roots of 1 then any central division algebra of degree p over F has an abelian splitting field. This implies that any central division algebra of degree p over a field of characteristic $\neq p$ has a solvable splitting field of a very simple type. An extension of this result that is a consequence of an important theorem of Merkurjev and Suslin will be proved by Saltman.

2.13. Inflation and Restriction for Crossed Products

We now resume our study of the Brauer groups $\text{Br}(F)$ and $\text{Br}(E/F)$ where E is finite dimensional Galois over F . We derive first two preliminary results on semi-linear transformations of a vector space.

Lemma 2.13.1. *Let V be a vector space over the finite dimensional Galois extension field E/F . Suppose for each $\sigma \in G$ we have a σ -semi-linear transformation u_σ of V ($u_\sigma(ax) = (\sigma a)u_\sigma x$) such that*

$$u_1 = 1_V, \quad u_\sigma u_\tau = u_{\sigma\tau}, \quad \sigma, \tau \in G. \quad (2.13.2)$$

Let $V_0 = \{y \in V \mid u_\sigma y = y, \sigma \in G\}$. Then V_0 is an F -subspace of V and the canonical map $a \otimes y \rightsquigarrow ay$ of $V_{0E} = E \otimes_F V_0$ into V is an isomorphism.

Proof. The assertion amounts to the following: $V = EV_0$ and elements of V_0 that are F -independent are E -independent. That V_0 is an F -subspace is clear. It is clear also that for any $x \in V$, $y = \Sigma u_\sigma x \in V_0$. Now let (b_1, \dots, b_n) be a base for E/F . Then the elements

$$y_i = \sum_{\sigma \in G} u_\sigma(b_i x) = \Sigma(\sigma b_i)u_\sigma x \in V_0. \quad (2.13.3)$$

Now the matrix $(\sigma_j b_i), G = \{\sigma_1, \dots, \sigma_n\}, 1 \leq i \leq n$, is invertible (BA I, p. 292). Hence we can solve the system (2.13.3) for the $u_\sigma x$ and express these as E -linear combinations of the $y_i \in V_0$. In particular, since $u_1 = 1$, x is an E -linear combination of $y_i \in V_0$. Evidently this implies that $V = EV_0$. Next suppose $y_1, \dots, y_r \in V_0$ are F -independent. Then the standard Dedekind independence argument shows that these elements are E -independent. \square

If V is a finite dimensional vector space then Lemma 2.13.1 implies (and is equivalent to) a classical result on matrices due to Speiser [19]. This is

Lemma 2.13.4. *Let E/F be Galois with Galois group G and let $\sigma \rightsquigarrow M_\sigma$ be a map of G into $GL_m(E)$ such that*

$$M_{\sigma\tau} = M_\sigma(\sigma M_\tau), \quad \sigma, \tau \in G. \quad (2.13.5)$$

Then there exists an $N \in GL_m(E)$ such that

$$M_\sigma = N(\sigma N)^{-1}. \quad (2.13.6)$$

Proof. Let u_σ be the σ -semilinear transformation of an m dimensional vector space V/E having the matrix M_σ relative to a base (x_1, \dots, x_m) for V/E : $u_\sigma x_i = \sum_j \mu_{ji\sigma} x_j$ where $M_\sigma = (\mu_{ji\sigma})$. Then (2.13.5) implies that $u_\sigma u_\tau = u_{\sigma\tau}$. Also the fact that the $M_\sigma \in GL_m(E)$ implies that the u_σ are bijective and hence $u_1 = u_1 u_1$ implies $u_1 = 1$. Thus we can apply Lemma 2.13.1 to obtain a base (y_1, \dots, y_m) for V/E such that the $y_i \in V_0$. Hence $u_\sigma y_i = y_i$, $1 \leq i \leq m$,

and so the matrix of u_σ relative to (y_1, \dots, y_m) is the identity matrix. Then if N is the matrix expressing the y 's in terms of the x 's: $y_i = \sum \nu_{ji} x_j$, $N = (\nu_{ij})$ we have $1 = N^{-1} M_\sigma(\sigma N)$. Hence (2.13.6) holds. \square

We suppose next that V and V' are vector spaces over E and u and u' are σ -semilinear transformations of V and V' respectively. Consider $V \otimes_E V'$. The map $x \otimes x' \rightsquigarrow ux \otimes u'x'$ for $x \in V, x' \in V'$ is additive in both arguments and for $a \in E$,

$$\begin{aligned} u(ax) \otimes u'x' &= (\sigma a)ux \otimes u'x' = ux \otimes (\sigma a)u'x' \\ &= ux \otimes u'(ax') \end{aligned}$$

Hence we have a balanced product of V and V' and so we have a unique endomorphism $u \otimes u'$ of the additive group of $V \otimes_E V'$ such that

$$(u \otimes u')(x \otimes x') = ux \otimes u'x'. \quad (2.13.7)$$

This is σ -semilinear, since if $a \in E$, then

$$\begin{aligned} (u \otimes u')(a(x \otimes x')) &= (u \otimes u')(ax \otimes x') \\ &= u(ax) \otimes u'x' = (\sigma a)ux \otimes u'x' = \sigma a(ux \otimes u'x'). \end{aligned}$$

We shall now apply the foregoing results to the following problem. Let E/F be Galois with $\text{Gal } E/F = G$ and suppose \bar{E} is a subfield of E/F that is Galois with $\text{Gal } \bar{E}/F = \bar{G}$. Then we know that $H = \text{Gal } E/\bar{E} \triangleleft G$ and the restriction map $\sigma \rightsquigarrow \bar{\sigma} = \sigma|_{\bar{E}}$ is a homomorphism of G onto \bar{G} with kernel H so $\bar{G} \cong G/H$. Suppose we are given a crossed product $\bar{A} = (\bar{E}, \bar{G}, \bar{k})$. Then \bar{A} is split by \bar{E} and hence by E . Accordingly, \bar{A} is similar to a crossed product (E, G, k) . What is the relation between \bar{k} and k ? This is given in the following theorem which is due to Hasse ([33]).

Theorem 2.13.8 (Inflation Theorem). *Let E/F be finite dimensional Galois, \bar{E}/F a Galois subfield, $G = \text{Gal } E/F$, $\bar{G} = \text{Gal } \bar{E}/F$, $\sigma \rightsquigarrow \bar{\sigma} = \sigma|_{\bar{E}}$ the canonical homomorphism of G onto \bar{G} . Let $(\bar{E}, \bar{G}, \bar{k})$ be a crossed product of \bar{G} with factor set \bar{k} . Then*

$$k : (\sigma, \tau) \rightsquigarrow k_{\sigma, \tau} = \bar{k}_{\bar{\sigma}, \bar{\tau}} \quad (2.13.9)$$

is a factor set of G with values in E^ and*

$$(\bar{E}, \bar{G}, \bar{k}) \sim (E, G, k). \quad (2.13.10)$$

Proof. As in the proof of Theorem 2.7.1, we can identify $\bar{A} = (\bar{E}, \bar{G}, \bar{k})$ with $\text{End}_{\bar{D}^0} \bar{V}$ where V is an r dimensional vector space over a division algebra \bar{D}^0 and $[\bar{V} : \bar{E}] = m$, the index of \bar{A} ($[\bar{D} : F] = m^2$). Let $u_{\bar{\sigma}}, u_{\bar{\tau}}, \bar{\sigma}, \bar{\tau} \in \bar{G}$, be elements of \bar{A} such that

$$u_{\bar{\sigma}} \bar{a} = (\bar{\sigma} \bar{a}) u_{\bar{\sigma}}, \quad u_{\bar{\sigma}} u_{\bar{\tau}} = \bar{k}_{\bar{\sigma}, \bar{\tau}} u_{\bar{\sigma} \bar{\tau}} \quad (2.13.11)$$

$\bar{a} \in \bar{E}$. Then $u_{\bar{\sigma}}$ is a $\bar{\sigma}$ -semilinear transformation of \bar{V} over \bar{E} . Also σ is a $\bar{\sigma}$ -semilinear transformation of E/\bar{E} since $\sigma(\bar{a}a) = (\sigma(\bar{a}a)) = (\sigma\bar{a})(\sigma a) = (\bar{\sigma}\bar{a})(\sigma a)$ for $\bar{a} \in \bar{E}, a \in E$. Hence we have a $\bar{\sigma}$ -semilinear transformation u_{σ} of $V = E \otimes_{\bar{E}} \bar{V}$ over E such that

$$u_{\sigma}(a \otimes \bar{x}) = \sigma a \otimes u_{\bar{\sigma}}\bar{x} \quad (2.13.12)$$

$a \in E, \bar{x} \in \bar{V}$. Moreover, since σ is also a σ -semilinear transformation of E it follows from (2.13.12) that u_{σ} is a σ -semilinear transformation of V . By (2.13.12) we have

$$u_{\sigma}u_{\tau} = \bar{k}_{\bar{\sigma}, \bar{\tau}}u_{\sigma\tau}. \quad (2.13.13)$$

It follows that k defined by (2.13.9) that u_{σ} is a σ -semilinear transformation of V . By (2.13.12) we have

$$u_{\sigma}u_{\tau} = \bar{k}_{\bar{\sigma}, \bar{\tau}}u_{\sigma\tau}. \quad (2.13.14)$$

It follows that k defined by (2.13.9) is a G -factor set with values in E^* and $A = \sum_{\sigma \in G} Eu_{\sigma} \cong (E, G, k)$.

It remains to show that $(\text{End}_F V)^A \sim (\text{End}_F \bar{V})^{\bar{A}}$ since these algebras are similar to A^0 and \bar{A}^0 respectively (Theorem 4.11, p. 224 of BA II). Since $A = \sum Eu_{\sigma}$ it is clear that $(\text{End}_F V)^A \subset L = \text{End}_{\bar{E}} V$ and $(\text{End}_F V)^A = \{\ell \in \text{End}_{\bar{E}} V \mid u_{\sigma}\ell u_{\sigma}^{-1} = \ell, \sigma \in G\}$. Similarly $(\text{End}_F \bar{V})^{\bar{A}} = \{\bar{\ell} \in \text{End}_{\bar{E}} \bar{V} \mid \bar{u}_{\bar{\sigma}}\bar{\ell}\bar{u}_{\bar{\sigma}}^{-1} = \bar{\ell}, \bar{\sigma} \in \bar{G}\}$. Now $\alpha_{\sigma} : \ell \rightsquigarrow u_{\sigma}\ell u_{\sigma}^{-1}$ is a σ -semilinear transformation of L and $\alpha_1 = 1_L$. Hence if $B = (\text{End}_F V)^A$ then by Lemma 2.13.1, $L = EB \cong E \otimes_F B$. Similarly, if $\bar{B} = (\text{End}_F \bar{V})^{\bar{A}}$ and $\bar{L} = \text{End}_{\bar{E}} \bar{V}$ then $\bar{L} = \bar{E}\bar{B} \cong \bar{E} \otimes_F \bar{B}$. By definition, $V = E \otimes_{\bar{E}} \bar{V}$. Hence identifying \bar{V} with the corresponding subset $1 \otimes \bar{V}$ of V , any $\bar{\ell} \in \bar{L}$ has a unique extension to a linear transformation of V/E which we shall also denote as $\bar{\ell}$. In this way we can regard \bar{L} as a subset of L . Then $L = E\bar{L} \cong E \otimes_{\bar{E}} \bar{L}$. Hence if $(\bar{\ell}_1, \dots, \bar{\ell}_{m^2})$ is a base for \bar{L}/\bar{E} then this is also a base for L/E . Since $\bar{L} = \bar{E}\bar{B} \cong \bar{E} \otimes_F \bar{B}$ we may assume that $\bar{\ell}_i \in B$. Then any element of L can be written in one and only one way as $\ell = \sum a_i \bar{\ell}_i, a_i \in E$ and every element of \bar{L} has this form with the $a_i \in F$. The condition $\alpha_{\sigma}\ell = \ell$ for $\ell = \sum a_i \bar{\ell}_i$ is equivalent to $\sigma a_i = a_i, 1 \leq i \leq m^2$. Hence $B = \bar{B}$ or, more precisely, B is the set of extensions to linear transformations in V/E of the linear transformations of $\bar{V}/\bar{E} \in \bar{B}$. Hence $(\text{End}_F V)^A \cong (\text{End}_F \bar{V})^{\bar{A}}$ and $(\text{End}_F V)^A \sim (\text{End}_F \bar{V})^{\bar{A}}$ as required. \square

The crossed product $A = (E, G, k)$ defined by $\bar{A} = (\bar{E}, \bar{G}, \bar{k})$ is called the *inflation*, $\text{Inf}_{\bar{E} \rightarrow E} \bar{A}$. An important application of inflation is the following result due to Brauer ([32]).

Theorem 2.13.14. *Let A be central simple with $[A]^e = 1$ where e is not divisible by $\text{char } F$. Then $A \sim (E, G, k)$ where the $k_{\sigma, \tau}$ are e -th roots of unity.*

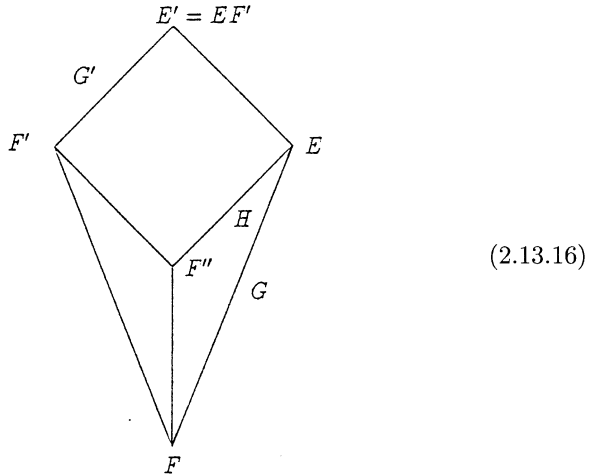
Proof. We may assume $A = (\bar{E}, \bar{G}, \bar{k})$ where \bar{E}/F is Galois with $\bar{G} = \text{Gal } \bar{E}/F$. Since $A^e \sim 1$ we have $\bar{\ell}_{\bar{\sigma}} \in \bar{E}$ such that $\bar{k}_{\bar{\sigma}, \tau}^e = \bar{\ell}_{\sigma}(\bar{\sigma}\bar{\ell}_{\tau})\bar{\ell}_{\bar{\sigma}}^{-1}$. Since e is not

divisible by $\text{char } \bar{E}$ the polynomials $\lambda^e - \bar{\ell}_\sigma$ are separable. Hence there exists an extension field E/\bar{E} such that E/F is finite dimensional Galois and E contains an e -th root ℓ_σ of $\bar{\ell}_\sigma$. Let $\text{Inf}_{\bar{E} \rightarrow E}(\bar{E}, \bar{G}, \bar{k})$ where $G = \text{Gal } E/F$ and k is as defined before. Consider

$$\varepsilon_{\sigma, \tau} = k_{\sigma, \tau} \ell_\sigma^{-1} (\sigma \ell_\tau)^{-1} \ell_{\sigma \tau}. \quad (2.13.15)$$

Then $\varepsilon_{\sigma, \tau}^e = 1$ and $(E, G, k) = (E, G, \varepsilon)$, $\varepsilon = \{\varepsilon_{\sigma, \tau}\}$. By the inflation theorem, $(\bar{E}, \bar{G}, \bar{k}) \sim (E, G, \varepsilon)$. \square

We investigate next the behavior of a crossed product under extension of the base field. Let E/F be Galois and let F' be any extension field of F (possibly infinite dimensional). Since E is a splitting field over F of a separable polynomial $f(\lambda) \in F[\lambda]$, the splitting field E'/F' of $f(\lambda)$ contains F' and E as subfields. Moreover, $E' = EF'$ and E' is Galois over F' . It is readily seen that up to isomorphism over F there is only one extension field E' of F containing E and F' as subfields and generated by E and F' . We call E' the *composite of E/F and F'/F* . Let $F'' = E \cap F'$.



Let $G' = \text{Gal } E'/F'$, $H = \text{Gal } E/F''$. If $\sigma' \in G'$ then $\sigma' \mid E \in H$ and the map $\sigma' \rightsquigarrow \sigma' \mid E$ is a homomorphism η of G' into H . We claim that this is an isomorphism. First, it is injective since $\eta(\sigma') = 1$ implies that $\sigma' \mid E = 1_E$ as well as $\sigma' \mid F' = 1_{F'}$. Then $\sigma' \mid E' = 1$ since $E' = EF'$. Thus $\sigma' = 1$. Next η is surjective. Otherwise $\text{Inv } \eta(G') \supsetneq E''$ whereas $\text{Inv } \eta(G') = \text{Inv } G' \cap E = F' \cap E = E''$. Hence η is an isomorphism. Then $[E' : F'] = G' = H = [E : F'']$. This implies that

$$E' = EF' \cong E \otimes_{F''} F'.$$

We can now prove the

Theorem 2.13.16 (Restriction Theorem, Hasse [33]). *Let E/F be finite dimensional Galois with Galois group G and let F' be an extension field of F , E' the composite of E and F' , $G' = \text{Gal } E'/F'$. Then for any factor set k of G into E^* we have*

$$(E, G, k)_{F'} \sim (E', G', k') \quad (2.13.17)$$

where

$$k'_{\sigma', \tau'} = k_{\sigma' | E, \tau' | E}, \quad \sigma', \tau' \in G'. \quad (2.13.18)$$

Proof. Let the notations be as above and put $A = (E, G, k)$. Then $A_{F'} = (A_{F''})_{F'}$. Since F'' is a subfield of E , hence of A , by Theorem 4.11 of BA II (p. 224), $A_{F''} \sim A^{F''}$. The latter has center F'' and a simple calculation shows that if $u_\sigma, \sigma \in G$, are the canonical generators for A over E then $A^{F''}$ is the subalgebra generated by E and the $u_\sigma, \sigma \in H$. It follows that $A^{F''} \cong (E, H, k_H)$ where k_H is the restriction of k to H . Then $A_{F''} \sim (E, H, k_H)$. Since $E' = EF' \cong E \otimes_{F''} F'$ it is clear that $(E, H, k_H)_{F'} \cong (E', G', k')$ where k' is given by (2.13.18). Hence $A_{F'} \sim (E', G', k')$. \square

The factor set k' is called the *restriction* of k and we have the *restriction homomorphism* $\text{Res} : [k] \rightsquigarrow [k']$ of $H^2(G, E^*)$ into $H^2(G', E'^*)$. We have the following commutative diagram

$$\begin{array}{ccc} H^2(G, E^*) & \longrightarrow & \text{Br}(E/F) \\ \downarrow & & \downarrow \\ H^2(G', E'^*) & \longrightarrow & \text{Br}(E'/F') \end{array} \quad (2.13.19)$$

where the horizontal maps are the isomorphisms $[k] \rightsquigarrow [(E, G, k)]$ and $[k'] \rightsquigarrow (E', G', k')$, the left vertical is Res and the right vertical is $[(E, G, k)] \rightsquigarrow [(E, G, k)_{F'}]$.

The two results we have derived specialize easily to the following results on cyclic algebras which we state without proofs.

Corollary 2.13.20. *Let E/F be cyclic with $\text{Gal } E/F = \langle \sigma \rangle$ and $[E : F] = n$. Let \bar{E} be the intermediate field with $[E : \bar{E}] = m$ and let $\bar{\sigma} = \sigma | \bar{E}$. Then $(\bar{E}, \bar{\sigma}, \gamma) \sim (E, \sigma, \gamma^m) (\cong (E, \sigma, \gamma) \otimes \cdots \otimes (E, \sigma, \gamma), m \text{ times})$.*

Corollary 2.13.21. *Let E/F be cyclic with $\text{Gal } E/F = \langle \sigma \rangle$ and let F' be an extension field of F . Suppose E' is the composite of E and F' , $[E' : F'] = m$, and σ' is the extension of $\sigma^{n/m}$ to E'/F' . Then $(E, \sigma, \gamma)_{F'} \sim (E', \sigma', \gamma)$.*

We remark that Albert's norm theorem (Lemma 2.10.1) is an immediate consequence of 2.13.20 and the theorem that $(E, \sigma, \gamma) \sim 1$ if and only if $\gamma = N_{E/F}(u)$ for some $u \in E$.

2.14. Isomorphism of $\text{Br}(F)$ and $H^2(F)$

We need to develop first some general results on the cohomology of groups. Let H and G be groups, σ a homomorphism of H into G . Then any G -module A (BA II, sec. 6.9) becomes an H -module via σ by defining the action of H on A by $(\sigma h)x, h \in H, x \in A$. Now suppose B is any H -module. Then a map s of A into B will be called *compatible with σ* if it is a module homomorphism of A as H -module into the H -module B . The condition for this is that for any $x \in A$ and any $h \in H$ we have

$$s((\sigma h)x) = h(sx). \quad (2.14.1)$$

Observe that if σ is bijective then this can be written also as $s(gx) = (\sigma^{-1}g)sx$ which is a generalization of the definition of σ^{-1} -semilinear transformation of one vector space into a second one. Now let $f \in C^n(G, A)$ the additive group of n -cochains with values in A . We can associate with f and the map s (compatible with σ) an n -cochain $\tilde{s}f$ of H with values in B defined by

$$\tilde{s}f(h_1, \dots, h_n) = sf(\sigma h_1, \dots, \sigma h_n), \quad h_i \in H. \quad (2.14.2)$$

Evidently $\tilde{s}: f \rightsquigarrow \tilde{s}f$ is a homomorphism of the additive group $C^n(G, A)$ into $C^n(H, B)$. Moreover, this commutes with the coboundary operator $f \rightsquigarrow \delta f$ where $\delta f \in C^{n+1}(G, A)$ is defined by

$$\begin{aligned} \delta f(g_1, \dots, g_{n+1}) &= g_1 f(g_2, \dots, g_{n+1}) \\ &+ \sum_{i=1}^n (-1)^i f(g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_{n+1}) \\ &+ (-1)^{n+1} f(g_1, \dots, g_n). \end{aligned} \quad (2.14.3)$$

The commutativity means that we have the commutative diagram:

$$\begin{array}{ccc} C^{(n)}(G, A) & \xrightarrow{\delta} & C^{(n+1)}(G, A) \\ s \downarrow & & \downarrow \tilde{s} \\ C^n(H, B) & \xrightarrow{\delta} & C^{n+1}(H, B) \end{array} \quad (2.14.4)$$

This follows directly from the definitions. As a consequence of this commutativity, we have an induced homomorphism of the cohomology group $H^n(G, A) = Z^n(G, A)/B^n(G, A)$ into $H^n(H, B)$ (BA II, loc. cit.).

One important special case of these considerations is that in which H is a subgroup of G , σ is the injection of H into G , A is a G -module and A is regarded as H -module via the injection i . Then the identity map is trivially an H -homomorphism of A as H -module with A as H -module. The corresponding homomorphism of $C^n(G, A)$ into $C^n(H, A)$ maps $f \in C^n(G, A)$ into $\tilde{i}f$ where $\tilde{i}f(h_1, \dots, h_n) = f(h_1, \dots, h_n)$. The corresponding homomorphism of $H^n(G, A)$ into $H^n(H, A)$ is called the *restriction homomorphism*.

Of particular interest for us is the case in which U and V are normal subgroups of G and $U \supset V$. We have the canonical homomorphism $gV \rightsquigarrow gU$ of G/V into G/U . Let A be a G -module and let $A^U(A^V)$ be the subset of A of elements x such that $ux = x, u \in U$ ($vx = x, v \in V$). Then A^U and A^V are submodules since $U \triangleleft G$ and these can be regarded in the natural way as G/U and G/V modules respectively. Evidently $A^U \subset A^V$ so we have the injection homomorphism of A^U into A^V (as additive groups). If $x \in A^U$ and $g \in G$ then

$$(gV)x = gx = (gU)x \quad (2.14.5)$$

which shows that the injection of A^U into A^V is compatible with the homomorphism of G/V into G/U . Hence we have the corresponding homomorphism, called the *inflation* $\text{inf}(U, V)$, of $H^n(G/U, A^U) \rightarrow H^n(G/V, A^V)$. This maps the cohomology class $f + B(G/U, A^U)$ into the class of the cocycle $f_{\text{inf}}(U, V)$ where

$$f_{\text{inf}(U, V)}(g_1V, \dots, g_nV) = f(g_1U, \dots, g_nU). \quad (2.14.6)$$

In the special case in which $V = 1$ so $G/V = G$ we have $f_{\text{inf}(U, 1)}$ given by

$$f_{\text{inf}}(g_1, \dots, g_n) = f(g_1U, \dots, g_nU). \quad (2.14.7)$$

We shall now apply this to Galois groups of possibly infinite Galois extension fields. Thus suppose \tilde{F}/F is algebraic, separable and normal over F . We shall be interested mainly in the case in which \tilde{F} is the separable algebraic closure F_s of F , that is, the subfield of separable elements of the algebraic closure \bar{F} of F . Let $G = \text{Gal } \tilde{F}/F$ with its usual topology (BA II, sec. 8.6). Let E/F be a finite dimensional Galois subfield of \tilde{F}/F and let $V = \text{Gal } \tilde{F}/E$. Then V is a closed normal subgroup of G which is the kernel of the restriction homomorphism $\sigma \rightsquigarrow \sigma|_E$. This is surjective so $\text{Gal } E/F = G/V$. Thus V has finite index and hence is open. Conversely, let V be any open normal subgroup of G . Then V is closed and G/V is discrete and compact. Hence G/V is finite and if $E = \text{Inv } V$ then E/F is finite dimensional Galois with $V = \text{Gal } \tilde{F}/E$. The multiplicative group E^* is a module for G/V and so we can define the cohomology groups $H^n(G/V, E^*)$. Now let K/F be a Galois subfield of E/F and let $U = \text{Gal } \tilde{F}/K$ so $V \subset U$. We have the inflation homomorphism $H^n(G/U, K^*) \xrightarrow{\text{inf}} H^n(G/V, E^*)$.

Let Σ be the set of finite dimensional Galois subfields of \tilde{F}/F . We partially order Σ by inclusion. Since any two finite dimensional Galois subfields of \tilde{F}/F are contained in a finite dimensional Galois subfield of \tilde{F}/F , Σ is a directed set. It is clear that the set of groups $H^n(G/V, E^*)$ together with the set of inflation maps between any two such groups determined by finite dimensional Galois subfield E and K with $E \supset K$ satisfy the conditions that permit defining the direct limit

$$H_c^n(G, \tilde{F}^*) = \varinjlim H^n(G/V, E^*)$$

(Theorem 2.8 of BA II). We call this group the n -th *continuous cohomology group of G with coefficients in \tilde{F}^** . We can also give a “global” definition of this

group. For this purpose we note that \tilde{F}^* is a continuous module for \tilde{G} in the sense that for fixed $a \in \tilde{F}^*$ the map $\sigma \rightsquigarrow \sigma a$ of G into \tilde{F}^* is continuous relative to the topology of \tilde{G} and the discrete topology of \tilde{F}^* . Now let $C_c^n(\tilde{G}, \tilde{F}^*)$ be the group of continuous maps of the n -fold product $G \times G \times \cdots \times G$ into \tilde{F}^* . The coboundary operator maps $C_c^n(G, \tilde{F}^*)$ into $C_c^{n+1}(G, \tilde{F})$ so we can define the corresponding cohomology groups. It is not difficult to show that these groups are isomorphic to the continuous cohomology groups defined as direct limits. We refer the reader to Serre's monograph *Cohomologie Galoisienne* ([64]) for a more complete discussion of continuous cohomology of profinite groups (= inverse limits of finite groups). The groups G are instances of such groups. For our purposes it will be convenient to use the definition by direct limits.

We shall now show that $H_c^2(G, \tilde{F}^*) \cong \text{Br}(\tilde{F}/F)$. We recall that if E/F is finite dimensional Galois the map $[k] \rightsquigarrow [(E, G, k)]$ is an isomorphism of $H^2(G, E^*)$ onto $\text{Br}(E/F)$ (Theorem 2.3.18) (iii)). If K/F is a Galois subfield of E/F and $V = \text{Gal } \tilde{F}/E$ and $U = \text{Gal } \tilde{F}/K$ then Theorem 2.13.8 implies the commutativity of the diagram

$$\begin{array}{ccc} H^2(G/U, K^*) & \longrightarrow & \text{Br}(K/F) \\ \text{Inf} \downarrow & & \downarrow \\ H^2(G/V, E^*) & \longrightarrow & \text{Br}(E/F) \end{array} \quad (2.14.8)$$

where the horizontal maps are the isomorphisms we have noted. Since every finite dimensional central simple algebra split by \tilde{F} is split by a finite dimensional Galois subfield of \tilde{F} , $\text{Br}(\tilde{F}/F) = \bigcup_{E \in \Sigma} \text{Br}(E/F)$. Thus $\text{Br}(\tilde{F}/F)$ can be regarded as a direct limit of the $\text{Br}(E/F)$. It follows readily from the commutativity of (2.14.8) and the definition of direct limits (BA II, p. 70) that we have

Theorem 2.14.9. $H_c^2(G, \tilde{F}^*) \cong \text{Br}(\tilde{F}/F)$.

The important special case of the foregoing theorem is that in which $\tilde{F} = F_s$, the separable algebraic closure of F . In this case we abbreviate $H_c^n(G, F_s^*)$ to $H^n(F)$. Moreover, since every finite dimensional central simple algebra has a separable splitting field, $\text{Br}(F_s/F) = \text{Br}(F)$. Hence we have

Corollary 2.14.10 $H^2(F) \cong \text{Br}(F)$.

Now let e be a positive integer not divisible by the characteristic of F . Let $\text{Br}_e(F)$ be the e -torsion part of $\text{Br}(F)$, that is, the subgroup of classes $[A]$ such that $[A]^e = 1$. Let μ_e denote the subgroup of the multiplicative group of \tilde{F}^* of e -th roots of 1. It is clear that $\mu_e \subset F_s$. By 2.13.14, if $[A] \in \text{Br}_e(F)$ then $[A] = [(E, G, k)]$ where the $k_{\sigma, \tau} \in \mu_e$. Let Σ_s be the set of finite dimensional Galois subfields of F_s that contain μ_e . If $E/F \in \Sigma_e$ and $V = \text{Gal } F_s/E$ then $\text{Gal } E/F \cong G/V$ where $G = \text{Gal } F_s/F$ and we have an induced action

on μ_e of the Galois action. Hence we can define $H^2(G/V, \mu_e)$ by this action. The isomorphism of $H^2(G/V, \mu_e)$ onto $\text{Br}_e(E/F) = \text{Br}(E/F) \cap \text{Br}_e(F)$. As in (2.14.8), we have the commutative diagram

$$\begin{array}{ccc} H^2(G/U, \mu_e) & \longrightarrow & \text{Br}_e(K/F) \\ \text{Inf} \downarrow & & \downarrow \\ H^2(G/V, \mu_e) & \longrightarrow & \text{Br}_e(E/F) \end{array} \quad (2.14.11)$$

if $K, E \in \Sigma_e$ and $K \subset E$. If we define $H_c^2(G, \varprojlim H^2(G/V, \mu_e))$ then the commutativity of (2.14.9) implies, as in the proof of Theorem 2.14.9 the following

Theorem 2.14.12. $H_c^2(G, \mu_e) \cong \text{Br}_e(F)$.

If $\mu_e \subset F$ then the action of G on μ_e is the trivial one and $H_c^2(G, \mu_e)$ is the usual continuous cohomology group of G with coefficients in μ_e .



<http://www.springer.com/978-3-540-57029-5>

Finite-Dimensional Division Algebras over Fields

Jacobson, N.

1996, VIII, 284 p., Hardcover

ISBN: 978-3-540-57029-5