THE BRAUER GROUP OF A FIELD

IGOR RAPINCHUK

This paper is devoted to the construction of the Brauer group of a field and its description in terms of factor sets. Since the elements of the Brauer group are similarity classes of central simple algebras over a given field, we begin by establishing some fundamental theorems for such algebras in §§1 and 2 (this material is contained, for example, in [2], [4] and [6]). In §3, we introduce the Brauer group of a field, and in §4 we describe it using factor sets and crossed products, which leads to an isomorphism between the Brauer group and a certain second cohomology group (this part closely follows the exposition given in [2], Ch. 4). In §5 we specialize to crossed products associated to cyclic Galois extensions. Finally, in §6 we apply the general theory to describe the Brauer group of a local field. (These two sections follow [4], Ch. 15 and 17.)

In this paper, all algebras will be associative and finite dimensional.

1. Basic facts about simple algebras

Let A be an algebra with identity over a field K. We recall that A is said to be *simple* if it has no proper two-sided ideals, and *central* if its center $Z(A)$ coincides with K. We will study algebras by analyzing the structure of modules over them. A (left) A-module M is *simple* if it contains no proper submodules. The following well-known statement will be used repeatedly.

Schur's Lemma. *If M and N are simple A-modules then every nonzero A-module homomorphism $f\colon M \to N$ is an isomorphism. In particular, if M is a simple A-module then* $\mathrm{End}_A\, M$ *is a division ring.*

Indeed, we have $\mathrm{Ker}\, f \neq M$, so $\mathrm{Ker}\, f = \{0\}$, and f is injective. Similarly, $\mathrm{Im}\, f \neq \{0\}$, so $\mathrm{Im}\, f = N$, making f also surjective, hence an isomorphism.

Now, let A be a (finite dimensional) simple K-algebra. By dimension consideration, there exists a minimal nonzero left ideal $M \subset A$. In the sequel, ${}_AA$ will denote A considered as a left A-module, and then M is a simple submodule of ${}_AA$.

Proposition 1. *Let A be a finite dimensional simple K-algebra, and $M \subset A$ be a nonzero minimal left ideal. Then*

(1) *there exists $n > 0$ such that ${}_AA \simeq \underbrace{M \oplus \cdots \oplus M}_{n}$ as A-modules;*

(2) *any A-module is isomorphic to a direct sum of copies of M, in particular M is the only simple A-module;*

(3) *let N_1 and N_2 be A-modules; then $N_1 \simeq N_2$ as A-modules if and only if $\dim_K N_1 = \dim_K N_2$ (we notice that any A-module has the natural structure of a K-vector space).*

Proof. (1): Since M is a left ideal, $\sum_{a\in A} Ma$ is a two-sided ideal, hence coincides with A. In particular, we can write

$$1 = m_1a_1 + \cdots + m_na_n \quad \text{with} \quad m_i \in M,\ a_i \in A,$$

and then

$$A = \sum_{i=1}^{n} Ma_n \tag{1}$$

We can assume that the set $\{a_1, \ldots, a_n\}$ is minimal with respect to the property $A = \sum Ma_i$, and then $Ma_i \neq \{0\}$ for all $i = 1, \ldots, n$. Notice that for any $a \in A$, the map $f_a \colon M \to Ma$, $x \mapsto xa$, is a surjective homomorphism of left A-modules. So, if $Ma \neq \{0\}$ then arguing as in the proof of Schur's Lemma, we see that f_a is injective, hence an isomorphism. Thus, all the Ma_i's in (1) are isomorphic to M, and in particular are simple A-modules. It remains to show that the sum (1) is direct. However, if for some j we have

$$Ma_j \bigcap \sum_{i \neq j} Ma_i \neq \{0\}$$

then because of the simplicity of Ma_j we conclude that $Ma_j \subset \sum_{i \neq j} Ma_i$. Then

$$A = \sum_{i \neq j} Ma_i,$$

contradicting the minimality of the set $\{a_1, \ldots, a_n\}$.

(2): Let N be a (nonzero) left A-module. Then N is a quotient of a free A-module which in combination with part (1) shows that there is a surjective homomorphism

$$f \colon \bigoplus_{i \in I} M_i \longrightarrow N$$

where each M_i is isomorphic to M. Set $N_i = f(M_i)$. We can discard those i for which $N_i = \{0\}$. Then clearly f gives an isomorphism between M_i and N_i, and in particular, N_i is simple. Furthermore, $N = \sum_{i \in I} N_i$, and it remains to find a subset $I_0 \subset I$ such that

$$N = \bigoplus_{i \in I_0} N_i. \tag{2}$$

For this we consider the collection $\mathcal{J}$ of all subset $J \subset I$ for which the sum $\sum_{i \in J} N_i$ is direct. Clearly, all one-element subsets of I belong to $\mathcal{J}$, in particular, $\mathcal{J} \neq \emptyset$. We can order $\mathcal{J}$ by inclusion, and then it is easy to see that $\mathcal{J}$ satisfies Zorn's Lemma. Let $I_0 \in \mathcal{J}$ be a maximal element provided by the latter. Then by our construction the sum $\sum_{i \in I_0} N_i$ is direct, and we only need to show that it coincides with N. Assume the contrary. Then in view of $N = \sum_{i \in I} N_i$, there exists $i_0 \in I$ such that $N_{i_0} \not\subset \sum_{i \in I_0} N_i$. Since N_{i_0} is simple, this actually means that $N_{i_0} \cap \sum_{i \in I_0} N_i = \{0\}$, implying that the sum $\sum_{i \in I_0 \cup \{i_0\}} N_i$ is also direct. This contradicts the maximality of I_0 and proves (2).

(3): We embed $K \hookrightarrow A$ by $x \mapsto x \cdot 1_A$, so any A-module can indeed be considered as a vector space over K. By part (2), we have

$$N_1 \simeq M^{\alpha_1} \quad \text{and} \quad N_2 \simeq M^{\alpha_2}$$

for some cardinal number numbers α_1 and α_2. Then

$$\dim_K N_i = (\dim_K M)\alpha_i,$$

and since $\dim_K M$ is finite, we see that

$$\dim_K N_1 = \dim_K N_2 \quad \Leftrightarrow \quad \alpha_1 = \alpha_2,$$

and our claim follows. □

Part (1) of Proposition 1 will enable us to prove Wedderburn's Theorem (see Theorem 1) which describes the structure of finite dimensional simple algebras. The argument will require the following.

Lemma 1. *Let A be an arbitrary ring, M be a left A-module, and $E = \mathrm{End}_A(M)$. Then for any $n \geqslant 1$, there exists a ring isomorphism*

$$\mathrm{End}_A(M^n) \simeq M_n(E), \tag{3}$$

the ring of $n \times n$-matrices over the ring E. Furthermore, if A is a K-algebra with identity then E, $\mathrm{End}_A(M^n)$, and $M_n(E)$ have the natural structures of a K-algebra for which (3) is an isomorphism of K-algebras.

Proof. Define $\varepsilon_i\colon M \to M^n$ and $\pi_i\colon M^n \to M$ by

$$\varepsilon_i\colon m \mapsto (0,\ldots,m,\ldots,0) \quad \text{and} \quad \pi_i\colon (m_1,\ldots,m_n) \mapsto m_i.$$

Then

$$\sum_{k=1}^n \varepsilon_k \pi_k = \mathrm{id}_{M^n} \qquad \text{and} \qquad \pi_k \circ \varepsilon_j = \mathrm{id}_M \ \text{ if } \ k = j \ \text{ and } \ 0 \ \text{ if } \ k \neq j.$$

Given $f \in \mathrm{End}_A(M^n)$, we let $f_{ij} = \pi_i \circ f \circ \varepsilon_j \in E$ for $i, j = 1, \ldots, n$. We claim that the correspondence

$$\mathrm{End}_A(M^n) \ni f \overset{\varphi}{\mapsto} (f_{ij}) \in M_n(E)$$

yields the required isomorphism (3). Indeed, for $f, g \in \mathrm{End}_A(M^n)$ we have

$$\varphi(f+g) = (\pi_i \circ (f+g) \circ \varepsilon_j) = (\pi_i \circ f \circ \varepsilon_j + \pi_i \circ g \circ \varepsilon_j) = (f_{ij}) + (g_{ij}) = \varphi(f) + \varphi(g),$$

and

$$\varphi(fg)_{ij} = \pi_i \circ f \circ \left(\sum_{k=1}^n \varepsilon_k \pi_k\right) \circ g \circ \varepsilon_j = \sum_{k=1}^n (\pi_i \circ f \circ \varepsilon_k)(\pi_k \circ g \circ \varepsilon_j) = \sum_{k=1}^n f_{ik} g_{kj} = (\varphi(f)\varphi(g))_{ij}$$

for all i, j, so $\varphi(fg) = \varphi(f)\varphi(g)$. Thus, φ is a ring homomorphism. Given $(f_{ij}) \in M_n(E)$, we define $f\colon M^n \to M^n$ by

$$f(m) = \left(\sum_{k=1}^n f_{1k}(\pi_k(m)), \ldots, \sum_{k=1}^n f_{nk}(\pi_k(m))\right).$$

Clearly, $f \in \mathrm{End}_A(M^n)$. Furthermore, for any i, j we have

$$(\pi_i \circ f \circ \varepsilon_j)(m) = \sum_{k=1}^n f_{ik}((\pi_k \circ \varepsilon_j)(m)) = f_{ij}(m),$$

showing that the correspondence $(f_{ij}) \mapsto f$ is inverse to φ and thus making φ a ring isomorphism.

As we observed in the proof Proposition 1, if A is a K-algebra, any A-module N becomes a K-vector space. Moreover, since K is contained in the center of A, $\mathrm{End}_A(N)$ becomes a K-algebra for the scalar multiplication

$$(af)(x) = f(ax) = af(x) \ \text{ for } \ a \in K, \ f \in \mathrm{End}_A(N), \ x \in N.$$

Since ε_i and π_j are A-module homomorphisms, we have

$$(af)_{ij} = \pi_i \circ (af) \circ \varepsilon_j = a(\pi_i \circ f \circ \varepsilon_j) = af_{ij},$$

which shows that (3) is an isomorphism of K-algebras. □

The following theorem is the main result of this section.

Theorem 1. (Wedderburn) *Let A be a finite dimensional simple algebra over a field K. Then $A \simeq M_n(D)$ for a unique $n \geqslant 1$ and a unique up to isomorphism division K-algebra D. Conversely, any algebra of the form $M_n(D)$, where D is a division algebra, is simple.*

Proof. We recall that the *opposite algebra* A^{op} is obtained by giving the same K-vector space A a new product defined by $a * b = ba$ where ba is the product in the original algebra A. First, we notice that $\mathrm{End}_A({}_AA) \simeq A^{\mathrm{op}}$. Indeed, if $\varphi \in \mathrm{End}_A({}_AA)$ then $\varphi(x) = x\varphi(1)$ for all $x \in A$, and then then the correspondence $\varphi \mapsto \varphi(1)$ yields the required isomorphism. On the other hand, by Proposition 1(1), for some $n \geqslant 1$, there is an isomorphism of left A-modules: ${}_AA \simeq M^n$, where M is a minimal nonzero left ideal of A. Then by Lemma 1, $\mathrm{End}_A({}_AA) \simeq M_n(E)$, where $E = \mathrm{End}_A(M)$. Since M is simple as A-module, E is a division algebra. Thus,

$$A^{\mathrm{op}} \simeq \mathrm{End}_A({}_AA) \simeq M_n(E).$$

It remains to observe that the map $a = (a_{ij}) \mapsto {}^t a = (a_{ji})$ gives an isomorphism $M_n(E)^{\mathrm{op}} \simeq M_n(E^{\mathrm{op}})$. So, we eventually obtain that $A \simeq M_n(D)$ with $D = E^{\mathrm{op}}$ (notice that the algebra opposite to a division algebra is itself a division algebra).

For the uniqueness of n and D, we need the following lemma.

Lemma 2. *Let $A = M_n(D)$, where D is a division ring, and let $V = D^n$ be the space of n-columns on which A acts by matrix multiplication on the left. Then V is a simple A-module and* $\mathrm{End}_A(V) \simeq D^{\mathrm{op}}$.

Proof. Given any nonzero $v, w \in V$, there exists $a \in A$ such that $av = w$, and the simplicity of V follows. Now, let $f \in \mathrm{End}_A(V)$. Let $v_0 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, and suppose that $f(v_0) = \begin{pmatrix} d \\ * \\ \vdots \\ * \end{pmatrix}$. We claim that $f(v) = vd$ for all $v \in V$. Indeed, let $v = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$. Then

$$f(v) = f\left(\begin{pmatrix} a_1 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ a_n & 0 & \dots & 0 \end{pmatrix} v_0\right) = \begin{pmatrix} a_1 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ a_n & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} d \\ \vdots \\ * \end{pmatrix} = vd.$$

Then the map $f \mapsto d$ gives the required isomorphism $\mathrm{End}_A(V) \simeq D^{\mathrm{op}}$. □

Now, suppose $A \simeq M_{n_1}(D_1)$ and $A \simeq M_{n_2}(D_2)$. Let $V_1 = D_1^{n_1}$ and $V_2 = D_2^{n_2}$. Then both V_1 and V_2 can be considered as A-modules. It follows form Lemma 2 that they are simple A-modules, and then by Proposition 1(2), they are isomorphic as A-modules. Using Lemma 2, we obtain

$$D_1^{\mathrm{op}} \simeq \mathrm{End}_A(V_1) \simeq \mathrm{End}_A(V_2) \simeq D_2^{\mathrm{op}},$$

so $D_1 \simeq D_2$ as K-algebras. Furthermore,

$$\dim_K A = n_1^2 \dim_K D_1 = n_2^2 \dim_K D_2,$$

so $n_1 = n_2$.

Finally, we need to show that $A = M_n(D)$, where D is a division algebra, is simple. Let e_{ij} be the standard basis of A. Suppose $\mathfrak{a} \subset A$ is a nonzero two-sided ideal, and pick a nonzero $a = (a_{ij}) \in \mathfrak{a}$ where, say, $a_{i_0j_0} \neq 0$. It is easy to check that

$$e_{ij} = e_{ii_0}(a_{i_0j_0}^{-1}a)e_{j_0j},$$

so $e_{ij} \in \mathfrak{a}$ for all i, j, and therefore $\mathfrak{a} = A$. □

Corollary 1. *Suppose K is an algebraically closed field. If A is a finite dimensional simple algebra over K then $A \simeq M_n(K)$ for some n.*

Indeed, it is enough to show that if D is a finite dimensional division algebra over K then $D = K$. Assume the contrary, and pick $a \in D \setminus K$. Then $K(a)/K$ is a nontrivial finite field extension, which cannot exist because K is algebraically closed. Thus, $D = K$.

The following statement is well-known.

Lemma 3. *Let $A = M_n(D)$. Then the center $Z(A)$ is naturally isomorphic to the center $Z(D)$.*

Indeed, if $a \in Z(A)$ then using the fact that a commutes with all elements of the standard basis e_{ij}, we immediately see that a is a scalar matrix. Furthermore, if α is its diagonal element then $\alpha \in Z(D)$. Conversely, any such scalar matrix is in $Z(A)$.

2. Fundamental theorems for simple algebras

The following simple facts will be used repeatedly.

Lemma 4. *Let V and W be vector spaces over a field K, and suppose $w_1, \dots, w_n \in W$ are linearly independent over K. If $a_1, \dots, a_n \in V$ are such that*

$$a_1 \otimes w_1 + \cdots + a_n \otimes w_n = 0 \quad \textit{in} \quad V \otimes_K W$$

then $a_1 = \cdots = a_n = 0$.

Proof. Being linearly independent, $w_1, \dots, w_n$ can be included in a basis $w_1, \dots, w_n, \dots$ of W. Let $v_1, \dots, v_m, \dots$ be a basis of V. We can write $a_i = \sum_j \alpha_{ij} v_j$ with $\alpha_{ij} \in K$, and then

$$0 = a_1 \otimes w_1 + \cdots + a_n \otimes w_n = \sum_i \left(\sum_j \alpha_{ij} v_j \right) \otimes w_i = \sum_{i,j} \alpha_{ij} (v_j \otimes w_i).$$

But it is well-known that the elements $v_j \otimes w_i$ form a basis of $V \otimes_K W$. So, all $\alpha_{ij} = 0$, and therefore $a_1 = \cdots = a_n = 0$. $\square$

If A and B are K-algebras then the tensor product of vector spaces $A \otimes_K B$ can be given a multiplication satisfying

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2,$$

and this multiplication makes $A \otimes_K B$ into a K-algebra. Furthermore, A and B can be identified with subalgebras of $A \otimes_K B$ by the maps $a \mapsto a \otimes_K 1_B$ and $b \mapsto 1_A \otimes b$, and then A and B commute inside $A \otimes_K B$. It is not difficult to see that $A \otimes_K B$ can in fact be characterized by the following universal property: given algebra homomorphisms $f\colon A \to C$ and $g\colon B \to C$ such that $f(A)$ and $g(B)$ commute inside C then there exists a unique algebra homomorphism $F\colon A \otimes_K B \to C$ such that $F(a \otimes b) = f(a)g(b)$.

Proposition 2. *For any two K-algebras A and B we have*

$$Z(A \otimes_K B) = Z(A) \otimes_K Z(B).$$

In particular, if A and B are central over K then so is $A \otimes_K B$.

Proof. The inclusion $\supset$ is obvious. To prove the opposite inclusion, take any $z \in Z(A \otimes_K B)$ and pick a shortest presentation of the form

$$z = \sum_{i=1}^{n} a_i \otimes b_i. \tag{4}$$

Then the systems $a_1, \dots, a_n$ and $b_1, \dots, b_n$ are linearly independent over K. Indeed, if $b_1, \dots, b_n$ are linearly dependent then one of them, say, b_1, is a linear combination of others:

$$b_1 = \beta_2 b_2 + \cdots + \beta_n b_n.$$

Then

$$z = a_1 \otimes (\beta_2 b_2 + \cdots + \beta_n b_n) + a_2 \otimes b_2 + \cdots + a_n \otimes b_n = (\beta_2 a_1 + a_2) \otimes b_2 + \cdots + (\beta_n a_1 + a_n) \otimes b_n$$

is a shorter presentation, a contradiction. Now, we claim that in (4), $a_1, \ldots, a_n \in Z(A)$ and $b_1, \ldots, b_n \in Z(B)$. Indeed, for any $a \in A$ we have

$$0 = (a \otimes 1)z - z(a \otimes 1) = \sum_{i=1}^{n} (aa_i - a_i a) \otimes b_i.$$

Since the b_i's are linearly independent, by Lemma 4, we have $aa_i - a_i a = 0$ for all $i = 1, \ldots, n$. Since $a \in A$ was arbitrary, we conclude that $a_i \in Z(A)$ for all i. The argument for $b_1, \ldots, b_n$ is similar. $\square$

The definition of the product on the Brauer group, which we will discuss in the next section, relies on the following statement.

Theorem 2. *Let A be a central simple K-algebra, and B be an arbitrary K-algebra. Then any two-sided ideal $\mathfrak{a} \subset A \otimes_K B$ is of the form $\mathfrak{a} = A \otimes_K \mathfrak{b}$ for some two-sided ideal $\mathfrak{b}$ of B. In particular, if B is also simple (but not necessarily central), then $A \otimes_K B$ is simple.*

Proof. We may assume that $\mathfrak{a} \neq \{0\}$. First, we will show that

$$\mathfrak{a} \bigcap B \neq \{0\}. \tag{5}$$

For this we pick a nonzero $x \in \mathfrak{a}$ which has a presentation of the form

$$x = \sum_{i=1}^{n} a_i \otimes b_i$$

with the smallest possible n. Then $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are linearly independent. In particular, $a_1 \neq 0$, so, since A is simple, we have $Aa_1A = A$, i.e. there exist $c_1, \ldots, c_\ell, d_1, \ldots, d_\ell \in A$ such that

$$c_1 a_1 d_1 + \cdots + c_\ell a_1 d_\ell = 1.$$

Consider

$$\tilde{x} = (c_1 \otimes 1)x(d_1 \otimes 1) + \cdots + (c_\ell \otimes 1)x(d_\ell \otimes 1) = (c_1 a_1 d_1 + \cdots + c_\ell a_1 d_\ell) \otimes b_1 + \cdots + (c_1 a_n d_1 + \cdots + c_\ell a_n d_\ell) =$$

$$= 1 \otimes b_1 + \tilde{a}_2 \otimes b_2 + \cdots + \tilde{a}_n \otimes b_n.$$

Clearly $\tilde{x} \in \mathfrak{a}$, $\tilde{x} \neq 0$ and $\tilde{x}$ has length $\leqslant n$. So, we may assume from the very beginning that $a_1 = 1$. We now claim that actually $n = 1$. Indeed, suppose $n \geqslant 2$. Since $a_1, \ldots, a_n$ are linearly independent over K, we have $a_2 \notin K = Z(A)$. So, there exists $a \in A$ such that $aa_2 \neq a_2 a$. Then

$$y = (a \otimes 1)x - x(a \otimes 1) = (aa_2 - a_2 a) \otimes b_2 + \cdots + (aa_n - a_n a) \otimes b_n$$

is a nonzero element in $\mathfrak{a}$ having length $< n$, a contradiction. So, $n = 1$, and $x = 1 \otimes b_1 \in \mathfrak{a}$, and (5) follows.

Thus, $\mathfrak{b} := \mathfrak{a} \cap B$ is a nonzero two-sided ideal of B. We claim that $\mathfrak{a} = A \otimes_K \mathfrak{b}$. In any case, $A \otimes_K \mathfrak{b}$ is a two-sided ideal of $A \otimes_K B$ contained in $\mathfrak{a}$. Then one can consider the canonical homomorphism

$$\varphi \colon A \otimes_K B \longrightarrow (A \otimes_K B)/(A \otimes_K \mathfrak{b}) \simeq A \otimes_K B/\mathfrak{b}$$

with $\mathrm{Ker}\ \varphi = A \otimes_K \mathfrak{b} \subset \mathfrak{a}$. If $\mathfrak{a} \neq A \otimes_K \mathfrak{b}$ then $\varphi(\mathfrak{a})$ is a nonzero two-sided ideal of $A \otimes_K B/\mathfrak{b}$. Applying (5) to the latter algebra, we obtain that $\varphi(\mathfrak{a}) \cap B/\mathfrak{b} \neq \{0\}$. Taking pullbacks, we obtain that for $\mathfrak{a} = \varphi^{-1}(\varphi(\mathfrak{a}))$ one has $\mathfrak{a} \cap B \supsetneqq \mathfrak{b}$, which contradicts our construction. $\square$

The proof of the following corollary requires one general remark: if A is a K-algebra then for any field extension L/K, the algebra $A_L := A \otimes_K L$ can be considered as an algebra over L for the scalar multiplication $\ell \cdot (a \otimes b) = a \otimes \ell b$, and $\dim_K A = \dim_L A_L$.

Corollary 2. *Let A be a finite dimensional central simple algebra over a field K. Then $\dim_K A$ is a perfect square.*

Proof. Let $\bar{K}$ be an algebraic closure of K. Consider $B := A \otimes_K \bar{K}$ as a $\bar{K}$-algebra. It follows from Theorem 2 that B is simple, and then by Corollary 1 we have $B \simeq M_n(\bar{K})$ for some $n \geqslant 1$. Thus,

$$\dim_K A = \dim_{\bar{K}} B = n^2.$$

□

The following theorem will enable us to construct the inverses of elements in the Brauer group.

Theorem 3. *Let A be a central simple algebra over a field K, $\dim_K A = n^2$. Then*

$$A \otimes_K A^{\mathrm{op}} \simeq \mathrm{End}_K(A) \simeq M_{n^2}(K).$$

Proof. For $a \in A$, define $\lambda_a \colon A \to A$ by $\lambda_a(x) = ax$. Clearly, $\lambda_a \in \mathrm{End}_K(A)$, and the correspondence $L \colon A \to \mathrm{End}_K(A)$, $a \mapsto \lambda_a$, is an algebra homomorphism. Similarly, for $b \in A$, we define $\rho_b \colon A \to A$ by $\rho_b(x) = xb$. Again, $\rho_b \in \mathrm{End}_K(A)$, and the correspondence $b \mapsto \rho_b$ defines an algebra homomorphism $R \colon A^{\mathrm{op}} \to \mathrm{End}_K(A)$. (The homomorphisms L and R are called the left and the right regular representations of A, respectively.) For any $a, b, x \in A$ we have

$$(\lambda_a \circ \rho_b)(x) = a(xb) = (ax)b = (\rho_b \circ \lambda_a)(x),$$

i.e. λ_a and ρ_b commute in $\mathrm{End}_K(A)$. Thus, there exists a homomorphism $F \colon A \otimes_K A^{\mathrm{op}} \to \mathrm{End}_K(A)$ which takes $a \otimes b$ to the endomorphism that acts as follows $x \mapsto axb$ (then an element $\sum a_i \otimes b_i$ corresponds to the endomorphism $x \mapsto \sum a_i x b_i$). By Theorem 2, the algebra $A \otimes_K A^{\mathrm{op}}$ is simple, so since F is not the zero homomorphism, we have $\mathrm{Ker}\, F = \{0\}$, i.e. F is injective. On the other hand,

$$\dim_K A \otimes_K A^{\mathrm{op}} = (n^2)^2 = \dim_K \mathrm{End}_K(A),$$

which implies that F is also surjective, hence an isomorphism. □

The following two theorems are the most important results about simple algebras.

Theorem 4. (Skolem-Noether) *Let A and B be finite dimensional simple K-algebras, with B central. If $f, g \colon A \to B$ are two K-algebra homomorphisms then there exists $b \in B^*$ such that*

$$g(a) = bf(a)b^{-1} \quad \textit{for all} \quad a \in A.$$

Proof. Consider $C = A \otimes_K B^{\mathrm{op}}$. Since B is central, B^{op} is also central, so it follows from Theorem 2 that C is simple. Associated with every homomorphism $f \colon A \to B$, one has a C-module structure on B given by

$$(a \otimes b)_f \cdot x = f(a)xb.$$

We will use B_f to denote B endowed with this structure. For our two homomorphisms $f, g \colon A \to B$, we obviously have $\dim_K B_f = \dim_K B_g$, so by Proposition 1(3) we have $B_f \simeq B_g$ as C-modules. Let $\varphi \colon B_f \to B_g$ be a C-module isomorphism. Set $b = \varphi(1)$. Then for any $x \in B$ we have

$$\varphi(x) = \varphi((1 \otimes x)_f \cdot 1) = (1 \otimes x)_g \cdot \varphi(1) = bx.$$

Applying the same argument to $\psi = \varphi^{-1} \colon B_g \to B_f$, we see that $\psi(x) = b'x$ where $b' = \psi(1)$. Then

$$x = (\varphi \circ \psi)(x) = bb'x,$$

so substituting $x = 1$, we get $bb' = 1$. Similarly, $b'b = 1$, i.e. $b \in B^*$. Furthermore, for any $a \in A$, we have

$$bf(a) = \varphi(f(a)) = \varphi((a \otimes 1)_f \cdot 1) = (a \otimes 1)_g \cdot \varphi(1) = g(a)b,$$

yielding $g(a) = bf(a)b^{-1}$, as required. □

Corollary 3. *Let A be a central simple algebra over K. Then every K-algebra automorphism of A is inner.*

Indeed, given a K-algebra automorphism $g\colon A \to A$, our claim follows from the theorem applied to $f = \mathrm{id}_A$. (A different proof based on Theorem 3 is given in [6], Ch. XI, Prop. 4.)

Theorem 5. (the Double Centralizer Theorem) *Let A be a central simple algebra over K of dimension $\dim_K A = n$, and let $B \subset A$ be a simple subalgebra of dimension $\dim_K B = m$. Denote*

$$Z_A(B) = \{x \in A \mid xb = bx \ \ \textit{for all} \ \ b \in B\}.$$

Then

(1) $Z_A(B) \otimes_K M_m(K) \simeq A \otimes B^{\mathrm{op}}$;

(2) $Z_A(B)$ *is a simple subalgebra of A of dimension* $\dim_K Z_A(B) = n/m$;

(3) $Z_A(Z_A(B)) = B$.

Proof. The proof is based on two simple observations that slightly generalize our previous constructions:

• In Proposition 2 we proved that for any K-algebras A and B one has $Z(A \otimes_K B) = Z(A) \otimes_K Z(B)$. The same argument shows that for any K-algebras A and B and any subalgebras $A' \subset A$ and $B' \subset B$ one has

$$Z_{A \otimes_K B}(A' \otimes_K B') = Z_A(A') \otimes_K Z_B(B').$$

• In the proof of Theorem 3, we constructed the representations $L\colon A \to \mathrm{End}_K(A)$, $a \mapsto \lambda_a$, and $R\colon A^{\mathrm{op}} \to \mathrm{End}_K(A)$, $b \mapsto \rho_b$, and observed that $L(A)$ and $R(A^{\mathrm{op}})$ commute inside $\mathrm{End}_K(A)$. In fact,

$$Z_{\mathrm{End}_K(A)}(L(A)) = R(A^{\mathrm{op}}).$$

Indeed, if $f \in Z_{\mathrm{End}_K(A)}(L(A))$ then $f(ax) = af(x)$ for all $a, x \in A$. Letting $x = 1$, we get $f(a) = af(1)$, i.e. $f = \rho_{f(1)}$.

To prove the theorem, we consider two embeddings $f, g\colon B \to A \otimes_K \mathrm{End}_K(B) = A \otimes_K M_m(K)$ given by

$$f(b) = b \otimes \mathrm{id}_B \ \ \text{and} \ \ g(b) = 1 \otimes \lambda_b.$$

We have

$$Z(A \otimes_K M_m(K)) = Z(A) \otimes_K Z(M_m(K)) = K \otimes_K K = K,$$

which means that $A \otimes_K M_m(K)$ is central. Then by the Skolem-Noether Theorem, f and g are conjugate, i.e. there exists $x \in (A \otimes_K \mathrm{End}_K(B))^*$ such that

$$f(b) = xg(b)x^{-1} \ \ \text{for all} \ \ b \in B.$$

This implies that

$$Z_{A \otimes_K \mathrm{End}_K(B)}(f(B)) = xZ_{A \otimes_K \mathrm{End}_K(B)}(g(B))x^{-1},$$

in particular, these centralizers are isomorphic. But

$$Z_{A \otimes_K \mathrm{End}_K(B)}(f(B)) = Z_{A \otimes_K \mathrm{End}_K(B)}(B \otimes_K K) = Z_A(B) \otimes_K \mathrm{End}_K(B)$$

and

$$Z_{A \otimes_K \mathrm{End}_K(B)}(g(B)) = Z_{A \otimes_K \mathrm{End}_K(B)}(K \otimes_K L(B)) = A \otimes_K R(B^{\mathrm{op}}).$$

Thus,

$$Z_A(B) \otimes_K \mathrm{End}_K(B) \simeq A \otimes_K B^{\mathrm{op}},$$

proving (1).

(2): By Theorem 2, the algebra $A \otimes_K B^{\mathrm{op}}$ is simple. So, the isomorphism in part (1) implies that $Z_A(B) \otimes_K \mathrm{End}_K(B)$ is simple, and therefore $Z_A(B)$ is simple. Counting dimensions, we obtain

$$\dim_K Z_A(B) \cdot m^2 = (\dim_K A) \cdot (\dim_K B) = nm.$$

So, $\dim_K Z_A(B) = n/m$ (in particular, m divides n).

(3): Obviously, $B \subset Z_A(Z_A(B))$. Applying part (2) to $Z_A(B)$ (which is simple), we obtain

$$\dim_K Z_A(Z_A(B)) = \frac{n}{\dim_K Z_A(B)} = \frac{n}{n/m} = m.$$

So, $B = Z_A(Z_A(B))$ by dimension considerations. □

Corollary 4. *Let A be a central simple algebra over K of dimension $\dim_K A = d^2$. If L is a field extension of K of degree ℓ then ℓ divides d and $Z_A(L)$ is a central simple algebra over L of dimension $\dim_L Z_A(L) = (d/\ell)^2$. In particular, if $\ell = d$ then $Z_A(L) = L$, and consequently, L is a maximal subfield of A.*

Proof. Since L is commutative, $L \subset Z_A(L)$. Then

$$\dim_K Z_A(L) = d^2/\ell = (\dim_L Z_A(L)) \cdot \ell,$$

so $\dim_L Z_A(L) = (d/\ell)^2$. Since

$$Z(Z_A(L)) \subset Z_A(Z_A(L)) = L,$$

we obtain that $Z_A(L)$ is central over L. □

Corollary 5. *Let D be a central division algebra over K of dimension $\dim_K D = d^2$. If $P \subset D$ is a maximal subfield then $\dim_K P = d$.*

Notice that every maximal subfield $P \subset D$ necessarily contains K as otherwise the subring generated by P and K would be a subfield of D strictly containing P. Furthermore, since D is finite dimensional, maximal subfields obviously exist. Now, let $P \subset D$ be a maximal subfield. Then $P = Z_D(P)$. Indeed, if $a \in Z_D(P) \setminus P$ then $P[a]$ would be a subfield strictly containing P. Applying the previous corollary, we obtain $\dim_K P = d$. (In this argument we used the obvious fact that any subalgebra of a finite dimensional division algebra is itself a division algebra.)

The following proposition is needed to give a cohomological interpretation of the Brauer group.

Proposition 3. *Let D be a central division algebra over a field K. Then D contains a maximal subfield P which is a separable extension of K.*

Proof. Of course, there is nothing to prove if K has characteristic zero or is finite. So, we can assume that K is an infinite field of characteristic $p > 0$. Next, it is enough to show that there always exists an element $a \in D \setminus K$ which is separable over K. Indeed, given this fact, we can complete the argument by induction on $\dim_K D = d^2$. Indeed, if $\ell = [K(a) : K] > 1$ then by Corollary 4, the centralizer $Z_D(K(a))$ is a central division algebra over $K(a)$ such that $\dim_{K(a)} Z_D(K(a)) = (d/\ell)^2 < \dim_K D$. Then by induction hypothesis, $Z_D(K(a))$ contains a maximal subfield P which is a separable extension of $K(a)$. Then P is a separable extension of K and by Corollary 5, $[P : K(a)] = d/\ell$, implying that $[P : K] = d$. Then by Corollary 4, P is a maximal subfield of D.

An element $a \in D \setminus K$ separable over K can be found in any maximal subfield P of D if d is not a power of p because in this case P/K cannot be purely inseparable (recall that the degree of a purely inseparable extension must be a power of p). So, we only need to consider the case where $d = p^\alpha$. Assume that $D \setminus K$ does not contain any elements separable over K. Then all these elements are purely inseparable, and since the degree of any element over K divides p^α, we obtain that $a^{p^\alpha} \in K$ for all

$a \in D$. Now, pick a basis $e_1 = 1, e_2, \ldots, e_{d^2}$ of D over K, and let $t_1, \ldots, t_{d^2}$ be variables. Then there exist polynomials $f_1, \ldots, f_{d^2} \in K[t_1, \ldots, t_{d^2}]$ such that

$$(t_1 e_1 + \cdots + t_{d^2} e_{d^2})^{p^\alpha} = f_1(t_1, \ldots, t_{d^2}) e_1 + \cdots f_{d^2}(t_1, \ldots, t_{d^2}) e_{d^2}.$$

Since $a^{p^\alpha} \in K$ for all $a \in D$, we have

$$f_2(a_1, \ldots, a_{d^2}) = \cdots = f_{d^2}(a_1, \ldots, a_{d^2}) = 0 \tag{6}$$

for all $(a_1, \ldots, a_{d^2}) \in K^{d^2}$. Then, because K is infinite, we conclude that $f_2 = \cdots = f_{d^2} = 0$, and therefore (6) for all $(a_1, \ldots, a_{d^2}) \in \bar{K}^{d^2}$. This means that $a^{p^\alpha} \in \bar{K}$ for all $a \in D \otimes_K \bar{K}$. But by Corollary 1, $D \otimes_K \bar{K} \simeq M_d(\bar{K})$, and for the element e_{11} of the standard basis we have $e_{11}^{p^\alpha} = e_{11} \notin \bar{K}$, a contradiction, proving the existence of separable elements. □

3. The Brauer group of a field

Two central simple algebras A_1 and A_2 are called *similar* (written $A_1 \sim A_2$) if the division algebras D_1 and D_2 such that $A_1 \simeq M_{n_1}(D_1)$ and $A_2 \simeq M_{n_2}(D_2)$, are isomorphic.

Lemma 5. (1) *For any K-algebra R, $R \otimes_K M_n(K) \simeq M_n(R)$;*

(2) *$M_m(K) \otimes_K M_n(K) \simeq M_{mn}(K)$;*

(3) *$A_1 \sim A_2$ if and only if there exist m_1 and m_2 such that $A_1 \otimes_K M_{m_1}(K) \simeq A_2 \otimes_K M_{m_2}(K)$;*

(4) *similarity is an equivalence relation.*

Proof. (1): There is an algebra homomorphism $R \otimes_K M_n(K) \to M_n(R)$ such that $r \otimes x \mapsto rx$. The inverse homomorphism is given by $(r_{ij}) \mapsto \sum_{i,j} r_{ij} \otimes e_{ij}$, where e_{ij} is the standard basis of M_n.

(2): We have a natural homomorphism

$$\mathrm{End}_K(K^m) \otimes_K \mathrm{End}_K(K^n) \to \mathrm{End}_K(K^m \otimes K^n) = \mathrm{End}_K(K^{mn}).$$

It is injective because it is nonzero and the algebra in the left-hand side is simple (Theorem 2), and it is then surjective by dimension count.

(3): Suppose $A_i \simeq M_{n_i}(D_i)$. If $A_1 \sim A_2$ then $D_1 \simeq D_2$ so using (1) and (2) we obtain

$$A_1 \otimes_K M_{n_2}(K) \simeq D_1 \otimes_K M_{n_1}(K) \otimes_K M_{n_2}(K) \simeq M_{n_1 n_2}(D_1) \simeq M_{n_1 n_2}(D_2) \simeq A_2 \otimes_K M_{n_1}(K).$$

Conversely, suppose $A_1 \otimes_K M_{m_1}(K) \simeq A_2 \otimes_K M_{m_2}(K)$. As above, we see that

$$A_i \otimes_K M_{m_i}(K) \simeq M_{m_i n_i}(D_i) \quad \text{for} \quad i = 1, 2.$$

So, by the uniqueness part of Theorem 1 we obtain that $D_1 \simeq D_2$, and $A_1 \sim A_2$.

(4): Follows immediately from the definitions. □

For a (finite dimensional) central simple algebra A over a field K, we let $[A]$ denote the equivalence class of algebras similar to A. As a set, the *Brauer group* of K (denoted $\mathrm{Br}(K)$) is the collection of all such classes (thus, the elements of $\mathrm{Br}(K)$ bijectively correspond to the isomorphism classes of central division algebras over K). We introduce a product on $\mathrm{Br}(K)$ by using tensor product of algebras:

$$[A][B] = [A \otimes_K B]. \tag{7}$$

We notice that the algebra $A \otimes_K B$ is central by Proposition 2 and simple by Theorem 2, so $[A \otimes_K B] \in \mathrm{Br}(K)$. If $A \sim A'$ and $B \sim B'$ then

$$A \otimes_K M_m(K) \simeq A' \otimes_K M_{m'}(K) \quad \text{and} \quad B \otimes_K M_n(K) \simeq B' \otimes_K M_{m'}(K)$$

for some integers m, m', n, n', and then

$$(A \otimes_K B) \otimes_K M_{mn}(K) \simeq (A' \otimes_K B') \otimes_K M_{m'n'}(K),$$

and therefore $A \otimes_K B \simeq A' \otimes_K B'$, by Lemma 5. This shows that the product operation (7) is well-defined. The associative and commutative properties for tensor product imply that this operation is, respectively, associative and commutative. Furthermore,

$$[A][M_n(K)] = [A \otimes_K M_n(K)] = [A],$$

so $[M_n(K)]$ is an identity element. Finally, using Theorem 3 we obtain that if $\dim_K A = n^2$ then

$$[A][A^{\mathrm{op}}] = [A \otimes_K A^{\mathrm{op}}] = [M_{n^2}(K)],$$

showing that $[A^{\mathrm{op}}]$ is an inverse element for $[A]$ in $\mathrm{Br}(K)$. Thus, we have proved the following.

Proposition 4. $\mathrm{Br}(K)$ *is an abelian group for the operation given by* (7).

We will analyze $\mathrm{Br}(K)$ by considering a system of its subgroups naturally associated with (finite) extensions of K. More precisely, let L/K be a field extension. For a central simple K-algebra A, we set $A_L = A \otimes_K L$. We say that L is a *splitting field* for A if $A_L \simeq M_n(L)$ as L-algebras. It is easy to see that if L splits A then L splits any algebra which is similar to A. The classes of algebras that split over a given extension L/K form a subgroup of $\mathrm{Br}(K)$ which is called the *relative Brauer group* associated with L/K and denoted $\mathrm{Br}(L/K)$. To see that $\mathrm{Br}(L/K)$ is indeed a subgroup of $\mathrm{Br}(K)$, we observe that it follows from Proposition 2 and Theorem 2 that for a central simple K-algebra A, the algebra A_L is a central simple L-algebra, and then the correspondence $[A] \mapsto [A_L]$ gives a well-defined map $\varepsilon_{L/K} \colon \mathrm{Br}(K) \to \mathrm{Br}(L)$. Moreover, there is an isomorphism of L-algebras

$$(A \otimes_K B) \otimes_K L \simeq (A \otimes_K L) \otimes_L (B \otimes_K L),$$

which shows that $\varepsilon_{L/K}$ is a group homomorphism. Clearly, $\mathrm{Br}(L/K)$ is precisely the kernel of this homomorphism, so in particular it is a subgroup of $\mathrm{Br}(K)$. We will now give an alternative characterization of the elements of $\mathrm{Br}(L/K)$ for finite extension L/K.

Theorem 6. *Let L/K be an extension of degree n.*

(1) *If A is a central simple K-algebra of dimension n^2 such that $L \subset A$ then $A_L \simeq M_n(L)$.*

(2) *Conversely, if a central simple K-algebra A splits over L then there exists a unique up to isomorphism central simple K-algebra A' such that $A \sim A'$, $\dim_K A' = n^2$ and $L \subset A'$.*

Thus, $\mathrm{Br}(L/K)$ *consists of the classes of central simple K-algebras that have dimension n^2 and contain L.*

Proof. (1): Consider A as a *right* vector space over L. Then for any $a \in A$, left multiplication $\lambda_a \colon A \to A$, $x \mapsto ax$, is an L-linear map of A. Since $\dim_L A = n$, the correspondence $a \mapsto \lambda_a$ defines a map

$$f \colon A \to \mathrm{End}_L(A) \simeq M_n(L),$$

which is easily seen to be a homomorphism of K-algebras. On the other hand, we have a homomorphism of K-algebras

$$g \colon L \to M_n(L), \quad x \mapsto \begin{pmatrix} x & & \\ & \ddots & \\ & & x \end{pmatrix}.$$

Clearly, the images of f and g commute, so there is a homomorphism of K-algebras

$$h \colon A \otimes_K L \to M_n(L) \ \text{ such that } \ h(a \otimes b) = f(a)g(b).$$

The simplicity of $A \otimes_K L$ implies that h is injective. Then, since

$$\dim_K A \otimes_K L = n^3 = \dim_K M_n(L),$$

we see that h is also surjective, and hence an isomorphism of K-algebras. Finally, for any $a \in A$ and $b, c \in L$ we have

$$h(c \cdot (a \otimes b)) = h(a \otimes cb) = f(a)cg(b) = cf(a)g(b) = c \cdot h(a \otimes b),$$

so h is actually an isomorphism of L-algebras.

(2): Let $A = M_d(D)$. Since L splits A, it also splits D. Indeed, if $D_L \simeq M_\ell(\Delta)$ where Δ is a division algebra then $A_L \simeq M_{d\ell}(\Delta)$, so from the uniqueness in Wedderburn's theorem we see that $\Delta = L$, and our claim follows. Thus, $D \otimes_K L \simeq M_m(L)$, where $m^2 = \dim_K D$. Then

$$D^{\mathrm{op}} \otimes_K L \simeq (D \otimes_K L)^{\mathrm{op}} \simeq M_m(L)^{\mathrm{op}} \simeq M_m(L), \tag{8}$$

i.e. L splits D^{op} as well. Let $V = L^m$. Because of the isomorphism (8), we can consider V as a left vector space over D^{op}. This is equivalent to considering V as a right vector space over D, so $\mathrm{End}_{D^{\mathrm{op}}}(V) \simeq M_t(D)$, where $t = \dim_{D^{\mathrm{op}}} V$. On the other hand, since L commutes with D^{op} inside $D^{\mathrm{op}} \otimes_K L \simeq M_m(L)$, the elements of L acts as D^{op}-endomorphisms of V, yielding an embedding of K-algebras $L \hookrightarrow M_t(D)$. Notice that

$$\dim_K V = mn = t \cdot \dim_K D,$$

implying that

$$t^2 \dim_K D = \frac{(mn)^2}{\dim_K D} = n^2.$$

Thus, $A' := M_t(D)$ has dimension n^2, is similar to A and contains an isomorphic copy of L, as required. Finally, the uniqueness of A' follows from the fact that because of dimension considerations, every class of similar algebras contains at most one algebra (up to isomorphism) of a given dimension. $\square$

We can now connect the (absolute) Brauer group $\mathrm{Br}(K)$ with the relative Brauer groups $\mathrm{Br}(L/K)$.

Proposition 5. $\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L/K)$ *where the union is taken over all finite Galois extensions of* K.

Proof. Let A be any central simple K-algebra. By Wedderburn's Theorem, $A \simeq M_d(D)$ where D is a division algebra. Using Proposition 3, we can find a maximal subfield P of D which is a separable extension of K. Then by Theorem 6 we have

$$D \otimes_K P \simeq M_\ell(P) \quad \text{where} \quad \dim_K D = \ell^2,$$

and therefore

$$A \otimes_K P \simeq (M_d(K) \otimes_K D) \otimes_K P \simeq M_d(P) \otimes_P D_P \simeq M_d(P) \otimes_P M_\ell(P) \simeq M_n(P)$$

with $n = d\ell$. On the other hand, since P is separable over K, its normal closure L is a (finite) Galois extension of K. Clearly,

$$A \otimes_K L \simeq (A \otimes_K P) \otimes_P L \simeq M_n(P) \otimes_P L \simeq M_n(L).$$

Thus, $[A] \in \mathrm{Br}(L/K)$, and the proposition follows. $\square$

4. $\mathrm{Br}(L/K)$ and factor sets

In this section, we fix a finite Galois extension L/K of degree n, and let $G = \mathrm{Gal}(L/K)$. By Theorem 6, every element of $\mathrm{Br}(L/K)$ is represented by a central simple K-algebra A of dimension n^2 which contains L. We begin by constructing a natural basis of A as a left vector space over L.

By the Skolem-Noether theorem, for every $\sigma \in G$, the identity embedding $L \hookrightarrow A$ is conjugate to the embedding $L \hookrightarrow A$ given by $a \mapsto \sigma(a)$, i.e there exists $x_\sigma \in A^*$ such that

$$x_\sigma a x_\sigma^{-1} = \sigma(a) \quad \text{for all} \quad a \in L. \tag{9}$$

Lemma 6. *$\{x_\sigma \mid \sigma \in G\}$ is a basis of A over L.*

Proof. Since $\dim_L A = n = |G|$, it is enough to show that these elements are linearly independent over L. Assume the contrary, and let

$$a_1 x_{\sigma_1} + \cdots a_r x_{\sigma_r} = 0$$

be the shortest possible relation of linear dependence (then in particular, all $a_i \neq 0$). Clearly, $r > 1$. Pick $\alpha \in L$ so that $L = K(\alpha)$; then $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ for $i \neq j$. We have

$$0 = \sigma_r(\alpha)(a_1 x_{\sigma_1} + \cdots a_r x_{\sigma_r}) - (a_1 x_{\sigma_1} + \cdots a_r x_{\sigma_r})\alpha =$$
$$= a_1(\sigma_r(\alpha) - \sigma_1(\alpha))x_{\sigma_1} + \cdots + a_{r-1}(\sigma_r(\alpha) - \sigma_{r-1}(\alpha))x_{\sigma_{r-1}},$$

which is a shorter relation of linear dependence, in which all the coefficients are $\neq 0$. A contradiction. $\square$

Thus,

$$A = \bigoplus_{\sigma \in G} L x_\sigma.$$

Notice that for any $a_\sigma, a_\tau \in L$ we have

$$(a_\sigma x_\sigma)(a_\tau x_\tau) = (a_\sigma x_\sigma a_\tau x_\sigma^{-1}) x_\sigma x_\tau = (a_\sigma \sigma(a_\tau)) x_\sigma x_\tau.$$

So, to understand multiplication in A, it is enough to describe the products $x_\sigma x_\tau$ for all $\sigma, \tau \in G$. For this, we compute the action of these products on L. For any $a \in L$, we have

$$(x_\sigma x_\tau) a (x_\sigma x_\tau)^{-1} = x_\sigma (x_\tau a x_\tau^{-1}) x_\sigma^{-1} = \sigma(\tau(a)) = (\sigma\tau)(a) = x_{\sigma\tau} a x_{\sigma\tau}^{-1}.$$

It follows that $c_{\sigma,\tau} := x_{\sigma\tau}^{-1} x_\sigma x_\tau$ centralizes L, and therefore $c_{\sigma,\tau} \in L^*$ by Corollary 4. Now, we can write

$$x_\sigma x_\tau = x_{\sigma\tau} c_{\sigma,\tau} = a_{\sigma,\tau} x_{\sigma\tau} \quad \text{with} \quad a_{\sigma,\tau} = x_{\sigma\tau} c_{\sigma,\tau} x_{\sigma\tau}^{-1} = (\sigma\tau)(c_{\sigma,\tau}) \in L^*.$$

Thus, multiplication in A is completely determined by specifying the elements $a_{\sigma,\tau} \in L^*$ for all $\sigma, \tau \in G$. The collection $\{a_{\sigma,\tau}\}$ is called a *factor set* of A relative to L; it is often convenient to view factor sets as functions $G \times G \to L^*$. These functions are not arbitrary: they must satisfy a system of relations derived from the associative law in A. To obtain these relations, take any $\rho, \sigma, \tau \in G$. Then

$$(x_\rho x_\sigma) x_\tau = (a_{\rho,\sigma} x_{\rho\sigma}) x_\tau = a_{\rho,\sigma}(x_{\rho\sigma} x_\tau) = a_{\rho,\sigma} a_{\rho\sigma,\tau} x_{(\rho\sigma)\tau}$$

and

$$x_\rho (x_\sigma x_\tau) = x_\rho (a_{\sigma,\tau} x_{\sigma,\tau}) = (x_\rho a_{\sigma,\tau} x_\rho^{-1})(x_\rho x_{\sigma\tau}) = \rho(a_{\sigma,\tau}) a_{\rho,\sigma\tau} x_{\rho(\sigma\tau)}.$$

Since $x_{(\rho\sigma)\tau} = x_{\rho(\sigma\tau)}$, we obtain that

$$\rho(a_{\sigma,\tau}) a_{\rho,\sigma\tau} = a_{\rho,\sigma} a_{\rho\sigma,\tau} \quad \text{for all} \quad \rho, \sigma, \tau \in G. \tag{10}$$

Notice that these conditions are identical to the conditions that define 2-cocycles on G with values in A^*, which allows us to treat every factor set as an element of the group of 2-cocycles $Z^2(G, L^*)$.

Now, let A' be a K-algebra isomorphic to A that also contains L (more precisely, we consider A and A' as K-algebras with fixed embeddings $\iota\colon L \hookrightarrow A$ and $\iota'\colon L \hookrightarrow A'$). Pick an arbitrary system of elements $\{x'_\sigma\}$ such that

$$x'_\sigma a (x'_\sigma)^{-1} = \sigma(a) \quad \text{for all} \quad a \in L,$$

and consider the corresponding factor set $\{a'_{\sigma,\tau}\}$ defined by

$$x'_\sigma x'_\tau = a'_{\sigma,\tau} x'_{\sigma\tau}. \tag{11}$$

We want to relate $\{a_{\sigma,\tau}\}$ and $\{a'_{\sigma,\tau}\}$. First, let $f\colon A \to A'$ be an arbitrary K-isomorphism. Then $f \circ \iota$ and ι' are two embeddings of L into A', so by the Skolem-Noether theorem there exists an invertible $t \in A'$ such that

$$(f \circ \iota)(a) = tat^{-1} \quad \text{for all} \quad a \in L^*.$$

Then $f' := i_{t^{-1}} \circ f$, where $i_{t^{-1}}$ is the inner automorphism of A' induced by t^{-1}, i.e. $i_{t^{-1}}(x) = t^{-1}xt$, has the property that $f' \circ \iota = \iota'$. This means that we can always choose our isomorphism $f \colon A \to A'$ so that it induces the identity map on L. Then for any $\sigma \in G$, we have in A' that

$$f(x_\sigma)af(x_\sigma)^{-1} = \sigma(a) = x'_\sigma a(x'_\sigma)^{-1} \text{ for all } a \in L.$$

So, $d_\sigma := f(x_\sigma)^{-1}x'_\sigma$ belongs to L^*, and we can therefore write

$$x'_\sigma = f(x_\sigma)d_\sigma = b_\sigma f(x_\sigma) \text{ with } b_\sigma = f(x_\sigma)d_\sigma f(x_\sigma)^{-1} = \sigma(d_\sigma) \in L^*.$$

Then

$$x'_\sigma x'_\tau = (b_\sigma f(x_\sigma))(b_\tau f(x_\tau)) = b_\sigma\sigma(b_\tau)f(x_\sigma x_\tau) = b_\sigma\sigma(b_\tau)a_{\sigma,\tau}f(x_{\sigma\tau}) = b_\sigma\sigma(b_\tau b_{\sigma\tau}^{-1})a_{\sigma,\tau}x'_{\sigma\tau}.$$

Comparing this with (11), we obtain

$$a'_{\sigma,\tau} = \frac{b_\sigma\sigma(b_\tau)}{b_{\sigma\tau}} \cdot a_{\sigma,\tau}. \tag{12}$$

Notice that functions of the form $b_\sigma\sigma(b_\tau)b_{\sigma\tau}^{-1}$ are precisely the elements of the group of 2-coboundaries $B^2(G, L^*)$. Thus, one can associate a well-defined element of $H^2(G, L^*)$ to every isomorphism class of central simple K-algebras A having dimension n^2 and containing L. Combining this with the fact that every element of $\mathrm{Br}(L/K)$ is represented by a unique up to isomorphism such algebra, we obtain a well-defined map

$$\beta_{L/K} \colon \mathrm{Br}(L/K) \longrightarrow H^2(G, L^*), \quad [A] \mapsto \{a_{\sigma,\tau}\}(\text{mod } B^2(G, L^*))$$

Lemma 7. *$\beta_{L/K}$ is injective.*

Proof. Let A and A' be two central simple K-algebras having dimension n^2 and containing L. Suppose they are written in the form

$$A = \bigoplus_{\sigma \in G} Lx_\sigma \quad \text{and} \quad A' = \bigoplus_{\sigma \in G} Lx'_\sigma$$

where the elements x_σ and x'_σ satisfy

$$x_\sigma a x_\sigma^{-1} = \sigma(a) \text{ and } x'_\sigma a(x'_\sigma)^{-1} = \sigma(a) \text{ for all } a \in L.$$

The corresponding factor sets $a_{\sigma,\tau}$ and $a'_{\sigma,\tau}$ are defined by

$$x_\sigma x_\tau = a_{\sigma,\tau}x_{\sigma\tau} \text{ and } x'_\sigma x'_\tau = a'_{\sigma,\tau}x'_{\sigma\tau}.$$

If $\beta_{L/K}([A]) = \beta_{L/K}([A'])$ then there exist elements $b_\sigma \in L^*$ for $\sigma \in G$ such that (12) holds. We want to show that A and A' are isomorphic. Define $f \colon A \to A'$ by

$$f\left(\sum_\sigma a_\sigma x_\sigma\right) = \sum_\sigma a_\sigma b_\sigma^{-1}x'_\sigma.$$

Clearly, f is an isomorphism of left vector spaces over L, and all we need to verify is that f is multiplicative. Because of the distributive law, it is enough to check that f is multiplicative on elements of the form $a_\sigma x_\sigma$. We have

$$f((a_\sigma x_\sigma)(a_\tau x_\tau)) = f((a_\sigma\sigma(a_\tau))a_{\sigma,\tau}x_{\sigma\tau}) = (a_\sigma\sigma(a_\tau))a_{\sigma,\tau}b_{\sigma\tau}^{-1}x'_{\sigma\tau}$$

and

$$f(a_\sigma x_\sigma)f(a_\tau x_\tau) = (a_\sigma b_\sigma^{-1}x'_\sigma)(a_\tau b_\tau^{-1}x'_\tau) = (a_\sigma\sigma(a_\tau)b_\sigma^{-1}\sigma(b_\tau^{-1}))x'_\sigma x'_\tau = (a_\sigma\sigma(a_\tau)b_\sigma^{-1}\sigma(b_\tau^{-1}))a'_{\sigma,\tau}x'_{\sigma\tau}.$$

It now follows from (12) that

$$f((a_\sigma x_\sigma)(a_\tau x_\tau)) = f(a_\sigma x_\sigma)f(a_\tau x_\tau),$$

as required. $\square$

Lemma 8. *$\beta_{L/K}$ is surjective.*

Proof. Let $\{a_{\sigma,\tau}\}$ be an arbitrary element of $Z^2(G, L^*)$, which means that (10) holds. Consider an n-dimensional left vector space over L with a basis $\{x_\sigma | \sigma \in G\}$:

$$A = \bigoplus_{\sigma \in G} Lx_\sigma.$$

Define a multiplication on A by the formula:

$$\left(\sum_\sigma a_\sigma x_\sigma\right)\left(\sum_\tau b_\tau x_\tau\right) = \sum_{\sigma,\tau} a_\sigma \sigma(b_\tau) a_{\sigma,\tau} x_{\sigma\tau}.$$

It is easy to see that this multiplication is K-bilinear and satisfies the distributive law, making A a K-algebra. We claim that A is a central simple K-algebra and $\beta_{L/K}([A]) = \{a_{\sigma,\tau}\}$. We will divide the verification into several small steps.

• *A is associative.* Because of the distributive law, it is enough the associative law only for elements of the form $a_\sigma x_\sigma$. A direct computation shows that

$$((a_\rho x_\rho)(a_\sigma x_\sigma))(a_\tau x_\tau) = (a_\rho \rho(a_\sigma)(\rho\sigma)(a_\tau)) a_{\rho,\sigma} a_{\rho\sigma,\tau} x_{(\rho\sigma)\tau}$$

and

$$(a_\rho x_\rho)((a_\sigma x_\sigma))(a_\tau x_\tau)) = (a_\rho \rho(a_\sigma)(\rho\sigma)(a_\tau)) \rho(a_{\sigma,\tau}) a_{\rho,\sigma\tau} x_{\rho(\sigma\tau)}.$$

Then (10) shows that these product are equal.

• $u := a_{1,1}^{-1} x_1$ *is an identity element for A.* Because of the distributive law, it is enough to check that

$$(a_\sigma x_\sigma)u = a_\sigma x_\sigma = u(a_\sigma x_\sigma) \tag{13}$$

For this we notice that plugging in σ for ρ and 1 for σ and τ in (10), we get

$$\sigma(a_{1,1}) a_{\sigma,1} = a_{\sigma,1} a_{\sigma,1},$$

i.e. $\sigma(a_{1,1}) = a_{\sigma,1}$. Then

$$(a_\sigma x_\sigma)u = (a_\sigma x_\sigma)(a_{1,1}^{-1} x_1) = (a_\sigma \sigma(a_{1,1})^{-1}) a_{\sigma,1} a_\sigma = a_\sigma x_\sigma,$$

verifying the first part of (13). The second part is verified similarly by observing that plugging in σ for τ and 1 for ρ and σ one gets $a_{1,\sigma} = a_{1,1}$.

It follows that L can be embedded in A by the map $a \mapsto au$.

• $x_\sigma^{-1} = (a_{\sigma^{-1},\sigma} a_{1,1})^{-1} x_{\sigma^{-1}}$, *in particular, x_σ is invertible.* Indeed, let $y = (a_{\sigma^{-1},\sigma} a_{1,1})^{-1} x_{\sigma^{-1}}$. Then

$$x_{\sigma^{-1}} x_\sigma = a_{\sigma^{-1},\sigma} x_1 = (a_{\sigma^{-1},\sigma} a_{1,1})u$$

proving that $yx_\sigma = u$. Furthermore,

$$x_\sigma y = \sigma(a_{\sigma^{-1},\sigma})^{-1} \sigma(a_{1,1})^{-1} x_\sigma x_{\sigma^{-1}} = \sigma(a_{\sigma^{-1},\sigma})^{-1} a_{\sigma,1}^{-1} a_{\sigma,\sigma^{-1}} x_1 = \sigma(a_{\sigma^{-1},\sigma})^{-1} a_{\sigma,1}^{-1} a_{\sigma,\sigma^{-1}} a_{1,1} u = u,$$

which follows from (10) by plugging in σ for ρ, σ^{-1} for σ and σ for τ, and using the fact that $a_{1,\sigma} = a_{1,1}$.

• $x_\sigma a x_\sigma^{-1} = \sigma(a)$ *for all $a \in L$.* We recall that $a \in L$ is identified with au, so we need to check that $x_\sigma(au)x_\sigma^{-1} = \sigma(a)u$. We have

$$x_\sigma(au)x_\sigma^{-1} = x_\sigma(aa_{1,1}^{-1} x_1)x_\sigma^{-1} = \sigma(a)\sigma(a_{1,1})^{-1} a_{\sigma,1} x_\sigma x_\sigma^{-1} = \sigma(a)u,$$

as required.

• *A is central over K.* For $a \in L$, we will write a instead of au. Suppose $z = \sum a_\sigma x_\sigma \in Z(A)$. Then for any $a \in L$ we have

$$a\left(\sum a_\sigma x_\sigma\right) = \sum a a_\sigma x_\sigma = \left(\sum a_\sigma x_\sigma\right) a = \sum a_\sigma \sigma(a) x_\sigma,$$

implying that $a_\sigma(a - \sigma(a)) = 0$ for all $\sigma \in G$. Pick a so that $L = K(a)$. Then for any $\sigma \neq 1$ we have $\sigma(a) \neq a$, so the above relation yields $a_\sigma = 0$. Thus, $z \in L$. But then $x_\sigma z x_\sigma^{-1} = \sigma(z) = z$ for any $\sigma \in G$, so $z \in K$.

• *A is simple.* Let $\mathfrak{a} \subset A$ be a nonzero two-sided ideal. Pick a nonzero element $a \in \mathfrak{a}$ which has the shortest presentation of the form

$$a = a_{\sigma_1} x_{\sigma_1} + \cdots + a_{\sigma_r} x_{\sigma_r};$$

then in particular all the coefficients are $\neq 0$. We claim that in fact $r = 1$. Assume that $r > 1$, and pick ℓ so that $L = K(\ell)$. Then $\sigma_i(\ell) \neq \sigma_j(\ell)$ for $i \neq j$, so

$$a\ell - \sigma_r(\ell)a = a_{\sigma_1}(\sigma_1(\ell) - \sigma_r(\ell))x_{\sigma_1} + \cdots + a_{\sigma_{r-1}}(\sigma_{r-1}(\ell) - \sigma_r(\ell))x_{\sigma_r}$$

is a nonzero in $\mathfrak{a}$ having a shorter presentation, a contradiction. Thus, $r = 1$, i.e. $a = a_{\sigma_1} x_{\sigma_1}$. But any nonzero element of this form is invertible, implying $\mathfrak{a} = A$.

Thus, A is a central simple algebra over K having dimension n^2 and containing L. By our construction, $x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau}$, which implies that

$$\beta_{L/K}([A]) = \{a_{\sigma,\tau}\} (\mathrm{mod}\ B^2(G, L^*)),$$

as required. □

The algebra A constructed in the proof of Lemma 8 is called the *crossed product* of L and G relative to the factor set $\{a_{\sigma,\tau}\}$ and will be denote $(L, G, \{a_{\sigma,\tau}\})$.

We are now in a position to prove the main result of this section.

Theorem 7. *$\beta_{L/K} \colon \mathrm{Br}(L/K) \to H^2(G, L^*)$ is a group isomorphism.*

Proof. It follows from Lemmas 7 and 8 that $\beta_{L/K}$ is a bijection, so all we need to show is that $\beta_{L/K}$ is a group homomorphism. For this we need to prove the following: let $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$ be two factor sets; consider the factor set $c_{\sigma,\tau} = a_{\sigma,\tau} b_{\sigma,\tau}$. Let

$$A = \bigoplus_\sigma L x_\sigma \quad , \quad B = \bigoplus_\sigma L y_\sigma \quad , \quad C = \bigoplus_\sigma L z_\sigma, \tag{14}$$

where

$$x_\sigma a x_\sigma^{-1} = y_\sigma a y_\sigma^{-1} = z_\sigma a z_\sigma^{-1} = \sigma(a) \ \text{ for all } \ a \in L$$

and

$$x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau} \quad , \quad y_\sigma y_\tau = b_{\sigma,\tau} y_{\sigma\tau} \quad , \quad z_\sigma z_\tau = c_{\sigma,\tau} z_{\sigma\tau},$$

be the corresponding crossed products. We need to show that

$$[C] = [A][B] = [A \otimes_K B].$$

We will show that in fact

$$A \otimes_K B \simeq M_n(C). \tag{15}$$

For this we consider $M = A \otimes_L B$ where both A and B are treated as left L-modules. Notice that $\dim_L A = \dim_L B = n$, so $\dim_L M = n^2$, and therefore $\dim_K M = n^3$. For any $a \in A$ and $b \in B$, the right multiplications by a and b define L-linear maps of A and B, respectively. It follows that one can give M a right $(A \otimes_K B)$-module structure such that

$$(x \otimes_L y)(a \otimes_K b) = xa \otimes_L yb.$$

Next, we will give M a left C-module structure using the canonical bases of A, B and C described in (14). We claim that there is a left C-module structure on M such that

$$(c_\sigma z_\sigma)(a \otimes_L b) = (c_\sigma x_\sigma a) \otimes_L y_\sigma b.$$

The left multiplications by $c_\sigma x_\sigma$ and y_σ are K-linear maps of A and B respectively, so there is a K-linear map $\gamma\colon A\otimes_K B\to A\otimes_K B$ such that $\gamma(a\otimes_K b)=(c_\sigma x_\sigma a)\otimes_K y_\sigma b$. On the other hand, M can be written as $(A\otimes_K B)/R$, where R is the K-vector subspace of $A\otimes_K B$ spanned by elements of the form $\ell a\otimes b-a\otimes \ell b$, for all $a\in A$, $b\in B$ and $\ell\in L$. Let us show that $\gamma(R)\subset R$. We have

$$\gamma(\ell a\otimes b-a\otimes \ell b)=c_\sigma x_\sigma \ell a\otimes y_\sigma b-c_\sigma x_\sigma a\otimes y_\sigma \ell b=\sigma(\ell)c_\sigma x_\sigma a\otimes y_\sigma b-c_\sigma x_\sigma a\otimes \sigma(\ell)y_\sigma b\in R,$$

as required. Thus, γ induces a K-linear map on M such that $\gamma(a\otimes b)=c_\sigma x_\sigma a\otimes y_\sigma b$, and this map is by definition the multiplication map by $c_\sigma z_\sigma$. This multiplication obviously extends to a map $C\times M\to M$ such that $(c_1+c_2)m=c_1m+c_2m$. It remains to verify that

$$c_1(c_2m)=(c_1c_2)m \tag{16}$$

It is enough to check this for elements of the form $c_1=c_\sigma z_\sigma$, $c_2=d_\tau z_\tau$ and $m=a\otimes_L b$. We have

$$c_1(c_2m)=(c_\sigma z_\sigma)(d_\tau x_\tau a\otimes_L y_\tau b)=c_\sigma x_\sigma d_\tau x_\tau a\otimes_L y_\sigma y_\tau b=c_\sigma\sigma(d_\tau)a_{\sigma,\tau}x_{\sigma\tau}a\otimes_L b_{\sigma,\tau}y_{\sigma\tau}b$$

and

$$(c_1c_2)m=(c_\sigma\sigma(d_\tau)c_{\sigma,\tau}z_{\sigma\tau})(a\otimes_L b)=c_\sigma\sigma(d_\tau)c_{\sigma,\tau}x_{\sigma\tau}a\otimes_L y_{\sigma\tau}b.$$

Since $c_{\sigma,\tau}=a_{\sigma,\tau}b_{\sigma,\tau}$, these expressions are equal, and we obtain (16). It is easy to see that

$$(cm)(a\otimes_K b)=c(m(a\otimes_K b)),$$

i.e. the left multiplication by C commutes with the right multiplication by $A\otimes_K B$. It follows that the right multiplication by $A\otimes_K B$ gives rise to a K-algebra homomorphism

$$(A\otimes_K B)^{\mathrm{op}}\xrightarrow{\varphi}\mathrm{End}_C(M).$$

Since $A\otimes_K B$, and hence $(A\otimes_K B)^{\mathrm{op}}$, is simple, φ is injective. To prove that it is also surjective, we compute the dimensions. We have

$$\dim_K M=n^3=\dim_K C^n,$$

so since C is simple, it follows from Proposition 1(3) that $M\simeq C^n$ as C-modules. So,

$$\mathrm{End}_C(M)\simeq M_n(C)^{\mathrm{op}}\simeq M_n(C^{\mathrm{op}}).$$

In particular,

$$\dim_K \mathrm{End}_C(M)=n^2\cdot\dim_K C=n^4=\dim_K A\otimes_K B,$$

implying that φ is surjective. Thus, φ is an isomorphism, so

$$A\otimes_K B\simeq(\mathrm{End}_C(M))^{\mathrm{op}}\simeq M_n(C),$$

proving (15), and completing the argument. □

Remark. A different proof of Theorem 7 is given in [3], §4.4.

We will now show that Theorem 7 can be extended to infinite Galois extensions. Let L/K be an infinite Galois extension with the Galois group $G=\mathrm{Gal}(L/K)$. Let $\{P_i\}_{i\in I}$ be a family of finite Galois extensions of K contained in L such that $L=\bigcup_{i\in I}P_i$, and for any $i,j\in I$ there exists $k\in I$ such that $P_i,P_j\subset P_k$. Then $G=\varprojlim G_i$ where $G_i=\mathrm{Gal}(P_i/K)=\mathrm{Gal}(L/K)/\mathrm{Gal}(L/P_i)$. We claim that

$$\mathrm{Br}(L/K)=\bigcup_{i\in I}\mathrm{Br}(P_i/K). \tag{17}$$

The inclusion $\supset$ is obvious. Let now $[A]\in\mathrm{Br}(L/K)$; then there exists an isomorphism of L-algebras $A\otimes_K L\overset{\alpha}{\simeq}M_n(L)$. Pick a basis $e_1,\dots,e_{n^2}$ of A over K. There exists $i\in I$ such that $\alpha(e_j)\in M_n(P_i)$ for all $j=1,\dots,n^2$, and then $\alpha(A)\subset M_n(P_i)$. Clearly, α induces an isomorphism of P_i-algebras $A\otimes_K P_i\simeq M_n(P_i)$. So, $[A]\in\mathrm{Br}(P_i/K)$, and (17) follows. We will interpret (17) as follows: for

$P_i \subset P_j$, there is the inclusion map $\iota_j^i\colon \mathrm{Br}(P_i/K) \to \mathrm{Br}(P_j/K)$; then $\{\mathrm{Br}(P_i/K), \iota_j^i\}$ is a direct system and

$$\mathrm{Br}(L/K) = \varinjlim\{\mathrm{Br}(P_i/K), \iota_j^i\}$$

On the other hand, for $P_i \subset P_j$, we have the natural surjective map $\rho_i^j\colon \mathrm{Gal}(P_j/K) \to \mathrm{Gal}(P_i/K)$ which gives rise to the inflation map

$$\theta_j^i\colon H^2(\mathrm{Gal}(P_i/K), P_i^*) \to H^2(\mathrm{Gal}(P_j/K), P_j^*),$$

which is defined by sending the class of a cocycle $\{a_{\sigma,\tau}\} \in Z^2(\mathrm{Gal}(P_i/K), P_i^*)$ to the class of the cocycle $\hat{a}_{\hat{\sigma},\hat{\tau}} \in Z^2(\mathrm{Gal}(P_j/K), P_j^*)$ given by

$$\hat{a}_{\hat{\sigma},\hat{\tau}} = a_{\rho_i^j(\hat{\sigma}),\rho_i^j(\hat{\tau})}.$$

Then by definition of the cohomology of profinite groups (cf. [1], Ch. V)

$$H^2(G, L^*) = \varinjlim\{H^2(\mathrm{Gal}(P_i/K), P_i^*), \theta_j^i\}.$$

For each i, by Theorem 7, we have an isomorphism $\beta_{P_i/K}\colon \mathrm{Br}(P_i/K) \to H^2(G_i, P_i^*)$. So, to construct an isomorphism $\beta_{L/K}\colon \mathrm{Br}(L/K) \to H^2(G, L^*)$, it is enough to show that the system $\{\beta_{P_i/K}\}$ defines an isomorphism between the direct systems $\{\mathrm{Br}(P_i/K), \iota_j^i\}$ and $\{H^2(\mathrm{Gal}(P_i/K), P_i^*), \theta_j^i\}$, i.e. if $P_i \subset P_j$ then the diagram

$$\begin{array}{ccc} \mathrm{Br}(P_i/K) & \xrightarrow{\iota_j^i} & \mathrm{Br}(P_j/K) \\ \beta_{P_i/K} \downarrow & & \downarrow \beta_{P_j/K} \\ H^2(G_i, P_i^*) & \xrightarrow{\theta_j^i} & H^2(G_j, P_j^*) \end{array}$$

is commutative; then we can set $\beta_{L/K} = \varinjlim \beta_{P_i/K}$.

Proposition 6. *Let $E \subset F$ be finite Galois extensions of K. Let $\iota\colon \mathrm{Br}(E/K) \to \mathrm{Br}(F/K)$ be the natural embedding, and let $\theta\colon H^2(\mathrm{Gal}(E/K), E^*) \to H^2(\mathrm{Gal}(F/K), F^*)$ be the inflation map. Then the diagram*

$$\begin{array}{ccc} \mathrm{Br}(E/K) & \xrightarrow{\iota} & \mathrm{Br}(F/K) \\ \beta_{E/K} \downarrow & & \downarrow \beta_{F/K} \\ H^2(\mathrm{Gal}(E/K), E^*) & \xrightarrow{\theta} & H^2(\mathrm{Gal}(F/K), F^*) \end{array}$$

is commutative.

Proof. Let $m = [E : K]$, $n = [F : K]$, $r = n/m$, and let $\rho\colon \mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K)$ be the canonical map. Any element of $\mathrm{Br}(E/K)$ is represented by an algebra A which is a crossed product $(E, \mathrm{Gal}(E/K), \{a_{\sigma,\tau}\})$ for some factor set $\{a_{\sigma,\tau}\}$. Then

$$A = \bigoplus_{\sigma \in \mathrm{Gal}(E/K)} E x_\sigma$$

where

$$x_\sigma a x_\sigma^{-1} = \sigma(a) \ \text{ for all } \ a \in E, \quad \text{and} \quad x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau}.$$

Then $\theta(\beta_{E/K}([A]))$ is represented by the cocycle $\hat{a}_{\hat{\sigma},\hat{\tau}}$ such that

$$\hat{a}_{\hat{\sigma},\hat{\tau}} = a_{\rho(\hat{\sigma}),\rho(\hat{\tau})}.$$

On the other hand, $\iota([A]) = [B]$ where $B = M_r(A)$. So, to prove our claim it is enough to write

$$B = \bigoplus_{\hat{\sigma} \in \mathrm{Gal}(F/K)} F y_{\hat{\sigma}}$$

where

$$y_{\hat{\sigma}} b y_{\hat{\sigma}}^{-1} = \hat{\sigma}(b) \ \text{ for all } \ b \in F, \quad \text{and} \quad y_{\hat{\sigma}} y_{\hat{\tau}} = \hat{a}_{\hat{\sigma},\hat{\tau}} y_{\hat{\sigma},\hat{\tau}}.$$

For this we pick a basis $e_1, \dots, e_r$ of F over E and embed F into $M_r(E) \subset B$ using the left regular representation λ which is described by

$$\lambda(b) = (s_{ij}) \quad \text{where} \quad be_j = \sum_{i=1}^{r} s_{ij} e_i.$$

Furthermore, for $\hat{\sigma} \in \mathrm{Gal}(F/K)$, we set

$$\mu(\hat{\sigma}) = (t_{ij}) \quad \text{where} \quad \hat{\sigma}(e_j) = \sum_{i=1}^{r} t_{ij} e_i.$$

Define an action of $\mathrm{Gal}(F/K)$ on $M_r(E)$ by

$$\hat{\sigma}((u_{ij})) = (\rho(\hat{\sigma})(u_{ij}))).$$

Then we have the following identities:

$$\mu(\hat{\sigma}\hat{\tau}) = \mu(\hat{\sigma})\hat{\sigma}(\mu(\hat{\tau})) \tag{18}$$

and

$$\lambda(\hat{\sigma}(b))\mu(\hat{\sigma}) = \mu(\hat{\sigma})\hat{\sigma}(\lambda(b)), \tag{19}$$

which are verified by direct computation (see [4, §14.5, Lemma] for the details). Clearly,

$$\hat{\sigma}(\lambda(b)) = \tilde{x}_{\hat{\sigma}} \lambda(b) \tilde{x}_{\hat{\sigma}}^{-1} \quad \text{where} \quad \tilde{x}_{\hat{\sigma}} = \mathrm{diag}(x_{\rho(\hat{\sigma})}, \dots, x_{\rho(\hat{\sigma})}),$$

so it follows from (19) that

$$\lambda(\hat{\sigma}(b)) = \mu(\hat{\sigma})\hat{\sigma}(\lambda(b))\mu(\hat{\sigma})^{-1} = \mu(\hat{\sigma})\tilde{x}_{\hat{\sigma}}\lambda(b)\tilde{x}_{\hat{\sigma}}^{-1}\mu(\hat{\sigma})^{-1}.$$

Thus, $y_{\hat{\sigma}} := \mu(\hat{\sigma})\tilde{x}_{\hat{\sigma}}$ satisfies

$$y_{\hat{\sigma}} b y_{\hat{\sigma}}^{-1} = \hat{\sigma}(b) \quad \text{for all} \quad b \in F.$$

Furthermore, using (18) we obtain

$$y_{\hat{\sigma}} y_{\hat{\tau}} = \mu(\hat{\sigma})\tilde{x}_{\hat{\sigma}}\mu(\hat{\tau})\tilde{x}_{\hat{\tau}} = \mu(\hat{\sigma})\hat{\sigma}(\mu(\hat{\tau}))x_{\hat{\sigma}}x_{\hat{\tau}} = \mu(\hat{\sigma}\hat{\tau})a_{\rho(\hat{\sigma}),\rho(\hat{\tau})}\tilde{x}_{\hat{\sigma}\hat{\tau}} = \hat{a}_{\hat{\sigma},\hat{\tau}} y_{\hat{\sigma}\hat{\tau}},$$

as required. □

It follows from Proposition 3 that $\mathrm{Br}(K) = \mathrm{Br}(K_{\mathrm{sep}}/K)$, where K_{sep} is a separable closure of K. Then we obtain the following.

Theorem 8. *For any Galois extension L/K, there is an isomorphism*

$$\beta_{L/K} \colon \mathrm{Br}(L/K) \longrightarrow H^2(\mathrm{Gal}(L/K), L^*).$$

In particular, $\mathrm{Br}(K) \simeq H^2(\mathrm{Gal}(K_{\mathrm{sep}}/K), K_{\mathrm{sep}}^*)$.

Now, let L/K be a finite Galois extension, and P be an intermediate subfield. Then $\mathrm{Gal}(L/P)$ is a subgroup of $\mathrm{Gal}(L/K)$, so there is the restriction map

$$\nu \colon H^2(\mathrm{Gal}(L/K), L^*) \to H^2(\mathrm{Gal}(L/P), L^*).$$

On the other hand, there is the homomorphism

$$\varepsilon \colon \mathrm{Br}(L/K) \to \mathrm{Br}(L/P), \quad [A] \mapsto [A \otimes_K P].$$

With these notations, we have the following.

Proposition 7. *The diagram*

$$\begin{array}{ccc} \mathrm{Br}(L/K) & \xrightarrow{\varepsilon} & \mathrm{Br}(L/P) \\ \beta_{L/K}\downarrow & & \downarrow\beta_{L/P} \\ H^2(\mathrm{Gal}(L/K), L^*) & \xrightarrow{\nu} & H^2(\mathrm{Gal}(L/P), L^*) \end{array}$$

is commutative.

Proof. Any element of $\mathrm{Br}(L/K)$ is represented by an algebra A which is a crossed product $(L, \mathrm{Gal}(L/K), \{a_{\sigma,\tau}\})$ for some factor set $\{a_{\sigma,\tau}\}$. Then

$$A = \bigoplus_{\sigma\in\mathrm{Gal}(L/K)} Lx_\sigma$$

where

$$x_\sigma a x_\sigma^{-1} = \sigma(a) \ \text{ for all } \ a \in L \ \text{ and } \ x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau}.$$

We already know that $Z_A(P)$ is a central simple P-algebra (Corollary 4), and clearly

$$Z_A(P) = \bigoplus_{\sigma\in\mathrm{Gal}(L/P)} Lx_\sigma.$$

It follows that

$$\nu(\beta_{L/K}([A])) = \beta_{L/P}([Z_A(P)]).$$

It remains to be shown that $[Z_A(P)] = [A \otimes_K P]$ in $\mathrm{Br}(L/P)$. For this, we consider A as a module over $A \otimes_K P^{\mathrm{op}} = A \otimes_K P$ with the scalar multiplication given by

$$(a \otimes p) \cdot b = abp.$$

As we have seen in the proof of the Double Centralizer Theorem, $\mathrm{End}_A({}_AA)$ consists of right multiplications by elements of A, hence is isomorphic to A^{op}. It follows that

$$\mathrm{End}_{A\otimes_K P}(A) \simeq Z_A(P)^{\mathrm{op}}$$

as P-algebras. On the other hand, since $A \otimes_K P$ is simple, we obtain from Proposition 1(3) that

$${}_{A\otimes_K P}A \otimes_K P \simeq A^r \ \text{ where } \ r = [P : K].$$

So,

$$(A \otimes_K P)^{\mathrm{op}} \simeq \mathrm{End}_{A\otimes_K P}({}_{A\otimes_K P}A \otimes_K P) \simeq M_r(\mathrm{End}_{A\otimes_K P}(A)) \simeq M_r(Z_A(P)^{\mathrm{op}})$$

It follows that $A \otimes_K P \simeq M_r(Z_A(P))$ as P-algebras, and therefore $[Z_A(P)] = [A \otimes_K P]$ in $\mathrm{Br}(L/P)$, as required. □

Corollary 6. *Let D be a central division algebra of dimension m^2 over K. Then $m[D]$ is trivial in* $\mathrm{Br}(K)$. *In particular,* $\mathrm{Br}(K)$ *is a periodic group.*

Indeed, pick a maximal subfield $P \subset D$ which is a separable extension of K, and let L be its Galois closure. Then $[D] \in \mathrm{Br}(L/K)$. On the other hand, by Theorem 6, $D \otimes_K P \simeq M_m(P)$. So, it follows from the proposition that $\nu(\beta_{L/K}([D]))$ is trivial, and therefore $\mu(\nu(\beta_{L/K}([D])))$ is trivial, where $\mu\colon H^2(\mathrm{Gal}(L/P), L^*) \to H^2(\mathrm{Gal}(L/K), L^*)$ is the corestriction map. But $\mu \circ \nu$ is multiplication by $m = [\mathrm{Gal}(L/K) : \mathrm{Gal}(L/P)]$ (cf. [1]), and our assertion follows.

5. Cyclic algebras

In this section, we specialize to the cases where L/K is a cyclic extension of degree n. Fix a generator σ of the Galois group $G = \mathrm{Gal}(L/K)$. Given a central simple algebra A over K of dimension n^2 that contains L, pick an arbitrary element $x_\sigma \in A^*$ such that

$$x_\sigma a x_\sigma^{-1} = \sigma(a) \quad \text{for all} \quad a \in L. \tag{20}$$

Set

$$x_{\sigma^i} = (x_\sigma)^i \quad \text{for} \quad i = 0, 1, \ldots, n-1.$$

Then $x_{\sigma^i} a x_{\sigma^i}^{-1} = \sigma^i(a)$ for all $i = 0, \ldots, n-1$. Let $\alpha = (x_\sigma)^n$.

Lemma 9. $\alpha \in K^*$.

Indeed, we have $(x_\sigma)^n a x_\sigma^{-n} = \sigma^n(a) = a$ implying that $\alpha = (x_\sigma)^n$ belongs to $Z_A(L) = L$. Furthermore,

$$\sigma(\alpha) = x_\sigma(x_\sigma^n)x_\sigma^{-1} = (x_\sigma)^n = \alpha,$$

yielding $\alpha \in K^*$.

Clearly, for $i, j \in \{0, \ldots, n-1\}$, we have

$$x_{\sigma^i} x_{\sigma^j} = \begin{cases} x_{\sigma^{i+j}} & , \quad i+j < n \\ \alpha x_{\sigma^{i+j-n}} & , \quad i+j \geqslant n \end{cases}$$

Thus, the multiplication table for A is completely determined by specifying α. We will denote this algebra by (L, σ, α). Using the definition $a_{\tau,\theta} = x_\tau x_\theta x_{\tau\theta}^{-1}$, we obtain that the corresponding factor set looks as follows:

$$a_{\sigma^i,\sigma^j} = \begin{cases} 1 & , \quad i+j < n \\ \alpha & , \quad i+j \geqslant n \end{cases}$$

We will denote this factor set by $\{a_{\sigma^i,\sigma^j}(\alpha)\}$. We have shown that any element of $\mathrm{Br}(L/K)$ is represented by an algebra of the form (L, σ, α) for some $\alpha \in K^*$. Because of the identification $\mathrm{Br}(L/K) \simeq H^2(G, L^*)$, this means that every element of $H^2(G, L^*)$ is represented by a cocycle $a_{\sigma^i,\sigma^j}(\alpha)$ for some $\alpha \in K^*$. Conversely, for any $\alpha \in K^*$, $a_{\sigma^i,\sigma^j}(\alpha)$ is a cocycle. Notice that

$$a_{\sigma^i,\sigma^j}(\alpha) a_{\sigma^i,\sigma^j}(\beta) = a_{\sigma^i,\sigma^j}(\alpha\beta) \quad \text{for any} \quad \alpha, \beta \in K^* \tag{21}$$

Any other element satisfying (20) is of the form $x'_\sigma = x_\sigma t$ for some $t \in L^*$, and then

$$\alpha' := (x'_\sigma)^n = (x_\sigma t) \cdots (x_\sigma t) = \sigma(t)\sigma^2(t) \cdots \sigma^n(t) x_\sigma^n = N_{L/K}(t)\alpha,$$

where $N_{L/K}$ is the norm map. Thus, the correspondence

$$\gamma_{L/K} \colon \mathrm{Br}(L/K) \to K^*/N_{L/K}(L^*), \quad [(L, \sigma, \alpha)] \mapsto \alpha N_{L/K}(L^*),$$

is well-defined. Conversely, if $\alpha' = \alpha N_{L/K}(t)$ then the correspondence $(x'_\sigma)^i \mapsto (x_\sigma t)^i$ for $i = 0, \ldots, n-1$, extends to an isomorphism of algebras $(L, \sigma, \alpha') \simeq (L, \sigma, \alpha)$, which shows that $\gamma_{L/K}$ is injective. Since $a_{\sigma^i,\sigma^j}(\alpha)$ is a cocycle for any $\alpha \in K^*$, we obtain from Lemma 8 that $\gamma_{L/K}$ is also surjective, hence bijective. Finally, using (21) and Theorem 7, we conclude that $\gamma_{L/K}$ is a group isomorphism. Thus, we have proved the following.

Theorem 9. *If L/K is a finite cyclic extension with the Galois group $G = \langle\sigma\rangle$, then the correspondence*

$$\gamma_{L/K} \colon \mathrm{Br}(L/K) \to K^*/N_{L/K}(L^*), \quad [(L, \sigma, \alpha)] \mapsto \alpha N_{L/K}(L^*),$$

is a group isomorphism.

Notice that this theorem gives an interpretation of the well-known isomorphism $H^2(G, L^*) \simeq K^*/N_{L/K}(L^*)$ for G cyclic, in the language of simple algebras.

Example 1. Take $K = \mathbb{R}$. Then $\mathrm{Br}(\mathbb{R}) = \mathrm{Br}(\mathbb{C}/\mathbb{R})$. By Theorem 9,

$$\mathrm{Br}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{R}^*/N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^*),$$

which is a group of order two. This means that there exist a unique up to isomorphism noncommutative central division algebra over $\mathbb{R}$. On the other hand, the algebra of Hamiltonian quaternions $\mathbb{H}$ is a central 4-dimensional division algebra over $\mathbb{R}$. Thus, we recover a theorem, due to Frobenius, that *any finite dimension central division algebra over* $\mathbb{R}$ *is isomorphic to* $\mathbb{H}$.

Example 2. Let $K = \mathbb{F}_q$ be a finite field with q element, and let $L = \mathbb{F}_{q^n}$. It is well-known that L/K is cyclic, and its Galois group is generated by the corresponding Frobenius automorphism. Then by Theorem 9

$$\mathrm{Br}(L/K) \simeq K^*/N_{L/K}(L^*).$$

But it is well-known that the norm map over finite fields is surjective. So, $\mathrm{Br}(L/K)$ is trivial for any finite extension L/K, and therefore $\mathrm{Br}(K)$ is trivial. This means that there are no noncommutative finite dimensional central division algebras over K. Since the center of any finite division division ring is a finite field, we recover a theorem, due to Wedderburn, that *any finite division ring is commutative.*

Before proceeding to our next example, we need to prove one lemma.

Lemma 10. *Let F/K be a cyclic extension of degree n with the Galois group* $\mathrm{Gal}(F/K) = \langle\hat{\sigma}\rangle$*, and let $E \subset F$ be a subextension having degree m over K and σ be the restriction of $\hat{\sigma}$ to F. Then for any $\alpha \in K^*$,*

$$(E, \sigma, \alpha) \sim (F, \hat{\sigma}, \alpha^r)$$

where $r = n/m$.

Proof. We will use the notations introduced in the proof of Proposition 6. It was shown therein that one can take $y_{\hat{\sigma}} = \mu(\hat{\sigma})\tilde{x}_{\hat{\sigma}}$. Then using (18) we obtain

$$y_{\hat{\sigma}}^n = (\mu(\hat{\sigma})\tilde{x}_{\hat{\sigma}}) \cdots (\mu(\hat{\sigma})\tilde{x}_{\hat{\sigma}}) = \mu(\hat{\sigma})\hat{\sigma}(\mu(\hat{\sigma})) \cdots \hat{\sigma}^{n-1}(\mu(\hat{\sigma}))\tilde{x}_{\hat{\sigma}}^n = \mu(\hat{\sigma}^n)(\tilde{x}_{\hat{\sigma}}^m)^r = \alpha^r$$

because $\mu(\hat{\sigma}^n)$ is the identity. □

Example 3. Let K be a local field, and K_n be its unramified extension of degree n. Then $\mathrm{Gal}(K_n/K)$ is generated by the corresponding Frobenius automorphism φ. It follows from Theorem 9 that the correspondence $[(K_n, \varphi, \alpha)] \mapsto \alpha N_{K_n/K}(K_n^*)$ gives an isomorphism $\gamma_{K_n/K} \colon \mathrm{Br}(K_n/K) \to K^*/N_{K_n/K}(K_n^*)$. It is well-known that $N_{K_n/K}(K_n^*) = UK^{*n}$ (cf. [5], Ch. V, §2), so the map $\alpha UK^{*n} \mapsto v(\alpha)/n$, where v is the valuation on K with the value group $\mathbb{Z}$, obviously gives a group isomorphism $K^*/N_{K_n/K}(K_n^*) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Composing it with $\gamma_{K_n/K}$, we get an isomorphism

$$i^{(n)} \colon \mathrm{Br}(K_n/K) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}, \quad (K_n, \varphi, \alpha) \mapsto v(\alpha)/n (\mathrm{mod}\ \mathbb{Z}).$$

Suppose now that $m|n$. Then $K_m \subset K_n$ and the restriction of the Frobenius automorphism $\hat{\varphi}$ of K_n to K_m gives the Frobenius automorphism φ of K_m. Then it follows from Lemma 10 that the diagram

$$\begin{array}{ccc} \mathrm{Br}(K_m/K) & \longrightarrow & \mathrm{Br}(K_n/K) \\ i^{(m)} \downarrow & & \downarrow i^{(n)} \\ \frac{1}{m}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \end{array}$$

in which the horizontal maps are standard embeddings, is commutative. It follows that for the maximal unramified extension K^{ur}, the Brauer group $\mathrm{Br}(K^{\mathrm{ur}}/K)$ is isomorphic to

$$\varinjlim \frac{1}{n}\mathbb{Z}/\mathbb{Z} = \mathbb{Q}/\mathbb{Z}.$$

6. The Brauer group of a local field

Let K be a local field, and v be the valuation on K. In this section, we will compute $\mathrm{Br}(K)$ through understanding the structure of finite dimensional central division algebras over K. So, let D be a central division algebra over K of dimension n^2. The first step in the analysis of the structure of D is extending the valuation to D. As in the case of fields, by a valuation on D we mean a map $w\colon D^* \to \mathbb{R}$ that satisfies the following two properties:

(V_1) $w(ab) = w(a) + w(b)$ for all $a, b \in D^*$;

(V_2) $w(a+b) \geqslant \min\{w(a), w(b)\}$ for all $a, b \in D^*$, $b \neq -a$.

We recall that given a field extension L/K of degree n, the valuation v has a unique extension to L which is given by the equation

$$\tilde{v}(\ell) = \frac{1}{n} v(N_{L/K}(\ell)) \ \text{ for all } \ \ell \in L^*. \tag{22}$$

A similar construction yields an extension of v to D, but the norm map $N_{L/K}$ needs to be replaced with the reduced norm map $Nrd_{D/K}$, which is defined as follows. Let P be any splitting field for D so that there exists an isomorphism $D \otimes_K P \overset{\varphi_P}{\simeq} M_n(P)$. Then we define

$$Nrd_{D/K}(a) = \det(\varphi_P(a \otimes 1)) \ \text{ for } \ a \in D^*.$$

The most important properties of this map are listed in the following proposition.

Proposition 8. (1) *$Nrd_{D/K}(a)$ is independent of the choice of P and φ_P.*

(2) *$Nrd_{D/K}$ defines a homomorphism of D^* to K^*;*

(3) *For any maximal subfield L of D, we have $Nrd_{D/K}(a) = N_{L/K}(a)$ for all $a \in L$.*

Proof. See [4], Ch. 16. □

Proposition 9. *The equation*

$$w(a) = \frac{1}{n} v(Nrd_{D/K}(a)) \tag{23}$$

defines a valuation on D that extends v.

Proof. Clearly, w extends v and satisfies (V_1), so we only need to verify (V_2). Take any $a, b \in D$, $b \neq -a$. Then $w(a+b) = w(a) + w(1 + a^{-1}b)$. Let L be a maximal subfield of D containing $a^{-1}b$. Then (22) defines an extension of v to L. On the other hand, for $\ell \in L$, using Proposition 8(3), we obtain

$$w(\ell) = \frac{1}{n} v(Nrd_{D/K}(\ell)) = \frac{1}{n} v(N_{L/K}(\ell)) = \tilde{v}(\ell).$$

So,

$$w(1+a^{-1}b) = \tilde{v}(1+a^{-1}b) \geqslant \min\{\tilde{v}(1), \tilde{v}(a^{-1}b)\} = \min\{w(1), w(a^{-1}b)\} = \min\{w(1), w(b) - w(a)\}.$$

Thus,

$$w(a+b) = w(a) + w(1+a^{-1}b) \geqslant w(a) + \min\{w(1), w(b) - w(a)\} = \min\{w(a), w(b)\},$$

as required. □

Let $\Gamma_w = w(D^*)$ and $\Gamma_v = v(K^*)$ be the value groups of w and v respectively. It follows from (23) that $n\Gamma_w \subset \Gamma_v$, so Γ_w is cyclic and the *ramification index* $e(D|K) = [\Gamma_w : \Gamma_v]$ is $\leqslant n$. Any element $\Pi \in D^*$ such that $w(\Pi)$ is the positive generator of Γ_w is called a *uniformizer.* As usual, $\mathcal{O}_w := \{a \in D^* | w(a) \geqslant 0\} \cup \{0\}$ is a subring of D, called the *valuation ring,* and $\mathfrak{P}_w := \{a \in D^* | w(a) > 0\} \cup \{0\}$ is a two-sided ideal of $\mathcal{O}_w$, called the *valuation ideal* of w. Clearly, $\mathfrak{P}_w = \Pi\mathcal{O}_w = \mathcal{O}_w\Pi$ for any uniformizer Π, and any element $a \in \mathcal{O}_w \setminus \mathfrak{P}_w$ is invertible in $\mathcal{O}_w$. It follows that $\bar{D} = \mathcal{O}_w/\mathfrak{P}_w$ is a division ring, called the *residue algebra.* It is an algebra over the residue field $k = \mathcal{O}_v/\mathfrak{p}_v$, where $\mathcal{O}_v$ and $\mathfrak{p}_v$ are the valuation ring and the valuation ideal in K. For $a \in \mathcal{O}_w$, we let $\bar{a}$ denote the image of a in $\bar{D}$. A standard argument shows that for $a_1, \ldots, a_r \in \mathcal{O}_w$, linear independence of $\bar{a}_1, \ldots, \bar{a}_r$ over k implies linear independence of $a_1, \ldots, a_r$ over K, which in particular implies that the *residual degree* $f(D|K) = \dim_k \bar{D}$ is finite.

Proposition 10. *We have $e(D|K) = f(D|K) = n$, and D contains an unramified extension of K of degree n.*

Proof. Since k and $f(D|K)$ are finite, the residue algebra $\bar{D}$ is finite, hence commutative by Wedderburn's theorem (Example 2 in §5). So, $\bar{D}$ is a finite field extension of k, and therefore $\bar{D} = k(\bar{a})$ for some $a \in \mathcal{O}_w$. Consider the field $L = K(a)$, and let E be the maximal unramified extension of K contained in L. Then for the corresponding residue fields we have $\bar{L} = \bar{E} = \bar{D}$. Since $[E : K] \leqslant n$, we obtain

$$f(D|K) = f(E|K) \leqslant n.$$

Now, let $\mathcal{O}(E)$ be the valuation ring of E. We claim that for any uniformizer $\Pi \in \mathcal{O}_w$ we have

$$\mathcal{O}_w = \mathcal{O}(E) + \mathcal{O}(E)\Pi + \cdots + \mathcal{O}(E)\Pi^{n-1}. \tag{24}$$

Let $\Lambda = \mathcal{O}(E) + \mathcal{O}(E)\Pi + \cdots + \mathcal{O}(E)\Pi^{n-1}$. Since $\mathcal{O}(E)$ is compact, Λ is also compact, hence closed in $\mathcal{O}_w$. So, to prove (24), it is enough to show that Λ is dense in $\mathcal{O}_w$, which is equivalent to

$$\mathcal{O}_w = \Lambda + \mathcal{O}_w\Pi^j \quad \text{for any} \quad j > 0.$$

But since $\bar{E} = \bar{D}$, we have $\mathcal{O}_w = \mathcal{O}(E) + \mathcal{O}(E)\Pi$. Iterating, we obtain

$$\mathcal{O}_w = \mathcal{O}(E) + \mathcal{O}(E)\Pi + \cdots + \mathcal{O}(E)\Pi^{j-1} + \mathcal{O}_w\Pi^j \quad \text{for any} \quad j > 0.$$

But Π satisfies an equation of degree n with coefficients in $\mathcal{O}_v$ and leading coefficient 1, so $\Pi^d \in \Lambda$ for any $d > 0$. This implies that

$$\mathcal{O}(E) + \mathcal{O}(E)\Pi + \cdots + \mathcal{O}(E)\Pi^{j-1} \subset \Lambda$$

for any j, and (24) follows. We then have

$$\mathcal{O}_w/\mathfrak{p}_v\mathcal{O}_w = \tilde{E} + \tilde{E}\tilde{\Pi} + \cdots + \tilde{E}\tilde{\Pi}^{n-1}, \tag{25}$$

where $\tilde{E}$ and $\tilde{\Pi}$ are the images of $\mathcal{O}(E)$ and Π in $\mathcal{O}_w/\mathfrak{p}_v\mathcal{O}_w$. Since E is unramified, we have $\tilde{E} = \bar{E}$, and $\dim_k \tilde{E} = f(D|K)$. Also, $\Pi^{e(D|K)} \in \mathfrak{p}_v\mathcal{O}_w$, so (25) reduces to

$$\mathcal{O}_w/\mathfrak{p}_v\mathcal{O}_w = \tilde{E} + \tilde{E}\tilde{\Pi} + \cdots + \tilde{E}\tilde{\Pi}^{e(D|K)-1}.$$

Taking the dimensions over k, we obtain $n^2 \leqslant e(D|K)f(D|K)$, so in fact $e(D|K) = f(D|K) = n$, and E is an unramified extension of K of degree n contained in D. ∎

Let K_n be the unramified extension of K of degree n, and K^{ur} be the maximal unramified extension of K. It follows from Proposition 10 that

$$\mathrm{Br}(K) = \bigcup_n \mathrm{Br}(K_n/K) = \mathrm{Br}(K^{\mathrm{ur}}/K).$$

On the other hand, as we have seen in Example 3 in §5, there is a system of compatible isomorphisms $i_K^{(n)} : \mathrm{Br}(K_n/K) \to (1/n)\mathbb{Z}/\mathbb{Z}$, leading to an isomorphism

$$i_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}, \quad [(K_n, \varphi_n, \alpha)] \mapsto v(\alpha)/n (\mathrm{mod}\ \mathbb{Z}),$$

where φ_n is the Frobenius automorphism of K_n/K. This proves the first assertion of the following theorem.

Theorem 10. (1) *There is an isomorphism* $i_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$.

(2) *If* L/K *is an extension of degree* n *then the diagram*

$$\begin{array}{ccc} \mathrm{Br}(K) & \xrightarrow{i_K} & \mathbb{Q}/\mathbb{Z} \\ \varepsilon_L \downarrow & & \downarrow \mu_n \\ \mathrm{Br}(L) & \xrightarrow{i_L} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{26}$$

where $\varepsilon_L([A]) = [A \otimes_K L]$ *and* μ_n *is multiplication by* n, *is commutative.*

Proof. We only need to prove assertion (2). First, we observe that if we have a tower of extensions $K \subset M \subset L$, and our assertion is true for the extensions M/K and L/M then it is also true for L/K. Since any extension L/K admits such a tower in which M/K is unramified and L/M is totally ramified, it is enough to consider separately the cases where L/K is unramified and totally ramified.

L/K is unramified. Any element of $\mathrm{Br}(K)$ is represented by an algebra $A = (K_m, \varphi_m, \alpha)$ where K_m/K is the unramified extension of degree m divisible by n and φ_m is the Frobenius automorphism of K_m. Recall that $\alpha = (x_{\varphi_m})^m$, where $x_{\varphi_m} \in A^*$ is an element such that $x_{\varphi_m} a x_{\varphi_m}^{-1} = \varphi_m(a)$ for all $a \in K_m^*$. Then

$$\mu_n(i_K([A])) = \frac{n v(\alpha)}{m} (\mathrm{mod}\ \mathbb{Z}). \tag{27}$$

Since $n|m$, we have $L \subset K_m$, and as we have seen in the proof of Proposition 7, $\varepsilon_L([A]) = [Z_A(L)]$. Besides, according to Corollary 4, $Z_A(L)$ is a central simple algebra over L of dimension $(m/n)^2$. The Frobenius automorphism of K_m/L is $(\varphi_m)^n$, and it is induced by the element $(x_{\varphi_m})^n \in Z_A(L)$. It follows that $Z_A(L) = (K_m, (\varphi_m)^n, \beta)$ where

$$\beta = ((x_{\varphi_m})^n)^{m/n} = (x_{\varphi_m})^m = \alpha.$$

So,

$$i_L(\varepsilon_L([A])) = v_L(\alpha)/(m/n) (\mathrm{mod}\ \mathbb{Z}), \tag{28}$$

where v_L is the valuation on L with the value group $\mathbb{Z}$. However, since L/K is unramified, we have $v_L(\alpha) = v(\alpha)$, and the commutativity of (26) follows from (27) and (28).

L/K is totally ramified. Again, consider an element of $\mathrm{Br}(K)$ which is represented by an algebra $A = (K_m, \varphi_m, \alpha)$. Then $\mu_n(i_K([A]))$ is still given by (27). Since L/K is totally ramified, we have $L \cap K_m = K$. As K_m/K is a Galois extension, we have $[K_m L : L] = [K_m : K]$, and therefore $[K_m L : K] = [K_m : K][L : K]$. It follows that the homomorphism $K_m \otimes_K L \to K_m L$, $a \otimes b \mapsto ab$, which is always surjective, is in fact an isomorphism. Thus, $A \otimes_K L$ contains $K_m L$ as a maximal subfield. The extension $K_m L/L$ is unramified of degree m, and its Frobenius automorphism $\tilde{\varphi}_m$ restricts to φ_m. It follows that the same element $x_{\varphi_m} \in A^* \subset (A \otimes_K L)^*$ induces $\tilde{\varphi}_m$. So, $A \otimes_K L = (K_m L, \tilde{\varphi}_m, \beta)$, where

$$\beta = (x_{\varphi_m})^m = \alpha.$$

Thus,

$$i_L(\varepsilon_L([A])) = v_L(\alpha)/m (\mathrm{mod}\ \mathbb{Z}). \tag{29}$$

But since L/K is totally ramified, we have $v_L(\alpha) = nv(\alpha)$. So, the commutativity of (26) follows from (27) and (29). $\square$

Corollary 7. *For any extension L/K of degree n, we have* $\mathrm{Br}(L/K) = \mathrm{Br}(K_n/K)$.

Indeed, it follows from the commutative diagram (26) that $\mathrm{Br}(L_1/K) = \mathrm{Br}(L_2/K) = i_K^{-1}(\mathrm{Ker}\, \mu_n)$ for any two extensions L_1/K and L_2/K of degree n.

Combining Corollary 7 with Example 3 in §5, we obtain

Corollary 8. *Let L/K be a Galois extension of degree n with the Galois group G. Then $H^2(G, L^*)$ is a cyclic group of order n.*

This result is crucial for local class field theory.

References

1. *Algebraic Number Theory,* edited by J.W.S. Cassels and A. Frölich, Acad. Press, 1967.
2. B. Farb, R.K. Dennis, *Noncommutative Algebra,* GTM 144, Springer, 1993.
3. I.N. Herstein, *Noncommutative Rings,* The Mathematical Association of America, 1994.
4. R.S. Pierce, *Associative Algebras,* GTM 88, Springer, 1982.
5. J-P. Serre, *Local Fields,* Springer, 1979.
6. A. Weil, *Basic Number Theory,* Springer, 1967.