The Brauer Group of a Nonarchimedean Local Field

Jon Hillery

December 9, 2022

Recall in our discussion of local class field theory that one of the key steps to understanding the abelian extensions L of a local field is understanding the second cohomology $H^2(\mathrm{Gal}(L/k), L^\times)$. As mentioned then, the importance of Brauer groups in class field theory comes from the fact that for any Galois extension of fields L/k we have that $H^2(\mathrm{Gal}(L/k), L^\times)$ is naturally isomorphic to the Brauer group $\mathrm{Br}(L/k)$, so Brauer groups provide a concrete way to calculate with cohomology. There will not be sufficient room to give a complete exposition of this story, but my aim will be to introduce the Brauer group independent of cohomology and then focus on the calculation we arrived at in our discussion of local class field theory:

Theorem 0.1

For K a nonarchimedean local field $\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$

Throughout, my reference unless otherwise specified will be the fourth chapter of [1].

§1 The Brauer Group

Definition 1.1. For an arbitrary field k, the **Brauer group $\mathrm{Br}(k)$** is the set of similarity classes of central simple finite-dimensional algebras over k, equipped with the group operation of tensor product.

Let's expand this definition and examine why it might be important. Throughout all k-algebras will assumed to be finite-dimensional over k. Recall that a k-algebra is **simple** if it contains no proper nontrivial two-sided ideals. We have already seen how the representation theory of k plays a role in abelian extensions, so it is already natural from the context of decomposability of representations to talk about simplicity and semi-simplicity of k-algebras. Simple algebras over a field have a nice classification:

Theorem 1.2

Every simple k-algebra A is isomorphic to a matrix ring $M_n(D)$ for some $n \in \mathbb{N}$ and D a division algebra.

Proof. The key idea of the proof is an extension of the fact that we can recover the scalars of a matrix ring over a commutative algebra from its center. Let S be a minimal nontrivial left ideal of A. Such an S exists because A and each of its ideals have finite dimension over k, ordering them by positive integers. We construct D as the **centralizer** of A in the k-algebra $\mathrm{End}_k(S)$, i.e. the set of elements of $\mathrm{End}_k(S)$ commuting with every element of A acting by left multiplication. This D is in fact a division algebra because the centralizer is closed under inverses (for $b \in D$, $ab = ba \implies a = bab^{-1} \implies b^{-1}a = ab^{-1}$) and $\mathrm{End}_k(S)$ is a division algebra: the kernel of k-linear $L : S \to S$ is a left ideal, either 0 or S by minimality, and so L is either invertible in $\mathrm{End}_k(S)$ or the zero map.

Now, we can re-write everything in terms of this constructed D. Since S is k-finite-dimensional we know that S is a finitely-generated D-module. For division algebras, that implies S is free over D: to any D-linearly-independent set $\{s_1, \dots, s_k\}$ when we adjoin any $s_{k+1} \notin \mathrm{Span}_D(s_1, \dots, s_k)$ then

$$d_1 s_1 + \cdots + d_{k+1} s_{k+1} = 0 \implies s_{k+1} = -d_{k+1}^{-1} \sum_{i=1}^{k} d_i s_i \implies d_{k+1}^{-1} d_i = 0 \implies d_i = 0$$

Therefore, we can indeed recover a matrix ring from endomorphisms of S: for a fixed basis $\{s_1, \dots, s_n\}$, any D-linear map $L : S \to S$ gives an element of $M_n(D)$ in the obvious way. Note that actually $\mathrm{End}_D(S) \cong M_n(D^{\mathrm{opp}})$ because if L_1, L_2 are given by matrices A, B then

$$L_1 L_2(s_i) = L_1 \left(\sum_j B_{j,i} s_j \right) = \sum_j B_{j,i} L_1 s_j = \sum_{j,k} B_{j,i} A_{k,j} s_k = \sum_{j,k} A_{k,j} \times_{\mathrm{opp}} B_{j,i} s_k$$

This is not a problem because D^{opp} is still a division algebra. To relate back to A, recall that D itself was defined as elements of $\mathrm{End}_k(S)$ commuting with A, and so a k-linear map $L : S \to S$ is D-linear exactly if it commutes with D. Thus, the theorem is completed by the "Double Centralizer Theorem": $A = C(C(A))$ in $\mathrm{End}_k(S)$ (where C denotes the centralizer operation), which we will now prove.

First, note that the map $A \to \mathrm{End}_k(S)$ to left-multiplication maps is truly an inclusion because its kernel is a two-sided ideal of the simple algebra k-algebra A (the kernel is proper because $1 \cdot s = s$). We have $A \subseteq C(C(A))$ because by definition of $d \in C(A)$, $ad(s) = da(s)$. Conversely, let $b \in C(C(A))$ and $\{v_1, \dots, v_k\}$ be a k-basis for S. Let $V = S \oplus \cdots \oplus S$ k times. If $L \in \mathrm{End}_k(V)$ is in the centralizer of A then it acts on the ith place by $(0, \dots, v, \dots, 0) \mapsto (L_{i,1} v, \dots, L_{i,n} v)$ where each component map is k-linear and commutes with the action of A, i.e. the centralizer of A in $\mathrm{End}_k(V)$ is exactly $M_n(D)$. Moreover, the centralizer of $M_n(D)$ is $C(C(A))$ (acting diagonally): for $c \in C(M_n(D))$, $c\delta_{i,j} = \delta_{i,j} c$ means c acts diagonally, and so on each factor it has to act by the centralizer of D, i.e. $C(C(A))$.

Let V_I be the submodule of V with zeroes in the entries outside $I \subseteq \{1, \dots, n\}$. Taking the maximal such V_I such that $A(v_1, \dots, v_k) \cap V_I = 0$ gives a direct sum decomposition $V = A(v_1, \dots, v_k) \oplus V_I$ because the intersection with any $V_{\{i\}}$ is either 0 or $V_{\{i\}}$ (by minimality of S) and if it were 0 then $V_{I \cup \{i\}}$ would contradict maximality of V_I. Thus, $V = A(v_1, \dots, v_k) \oplus W$ with A-linear projection π onto the first factor. By the last paragraph, the action of $C(C(A))$ diagonally is also the centralizer of A in $\mathrm{End}_k(V)$ and so

$$\pi b(v_1, \dots, v_k) = b\pi(v_1, \dots, v_k) = b(v_1, \dots, v_k) \implies b(v_1, \dots, v_k) \in A(v_1, \dots, v_k)$$

i.e. b acts by some $a \in A$, as desired. □

The next question is a natural group operation on these algebras, which is answered by the tensor product. For arbitrary division algebras D_1, D_2 it is true that $M_n(D_1) \otimes M_m(D_2) \cong M_{nm}(D_1 \otimes D_2)$ (see below), however the tensor product of simple algebras need not be simple: $\mathbb{C}$ is simple over $\mathbb{R}$ yet $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$ which has nontrivial ideals given by each factor. One solution is the requirement that our k-algebras be **central**, i.e. having center exactly k. In particular,

Lemma 1.3

The tensor product of two central simple algebras A, B over k is again central simple. In fact, only one of the algebras is required to be central.

Proof. Write the algebra assumed to be central as $M_n(D)$ and the other as A. By the usual change of scalars, $A \otimes_k M_n(D) = M_n(A \otimes_k D)$. If we can show that $A \otimes_k D$ is simple, then it is isomorphic to some $M'_n(D')$, and so we have $A \otimes_k M_n(D) \cong M_n(M_{n'}(D')) = M_{nn'}(D')$. This algebra is always simple because we can pick out any elements with the same elementary matrices as above, so the only two-sided ideals would be of the form $M_{nn'}(I)$ where I is a two-sided ideal of D'. Letting $\{A_i\}$ be a basis for $M_n(D)$ and $\{a_j\}$ a basis for A (bases over k), if $b = \sum_{i,j} k_{i,j} A_i \otimes a_j$ is in the center of $A \otimes_k M_n(D)$ then

$$(1 \otimes A_{i_0}) \left(\sum_{i,j} k_{i,j} a_j \otimes A_i \right) = \left(\sum_{i,j} k_{i,j} a_j \otimes A_i \right) (1 \otimes A_{i_0}) \implies \sum_{i,j} k_{i,j} a_j \otimes (A_{i_0} A_i - A_i A_{i_0}) = 0$$

$$\implies \sum_i k_{i,j} (A_{i_0} A_i - A_i A_{i_0}) = 0 \ \forall j, i_0 \implies \sum_i k_{i,j} A_i \in k \ \forall j$$

and similarly for the a_j, i.e. the center of $A \otimes_k M_n(D)$ is in fact k.

It remains to show that $A \otimes_k D$ is simple. Suppose I is a nontrivial two-sided ideal of $A \otimes_k D$. That means that I is also a D-submodule under the action $d \cdot (a \otimes_k d') = a \otimes_k dd'$. Our basis $\{a_j\}$ for A then leads to D-basis $\{a_j \otimes 1\}$. Following notation introduced by Bourbaki, let $J(a)$ be the subset of $j \in \{1, \ldots, n\}$ such that the $(a_j \otimes 1)$-coefficient of a (over D) is nonzero. We then say $a \in I$ is **primordial** with respect to this basis if $J(a)$ is minimal among nonzero elements $a \in I$ and at least one of the coefficients is 1. Because everything is finite-dimensional, such an a exists (to ensure a coefficient is 1, multiply a by the inverse of one of the nonzero coefficients). Now, choosing a fixed primordial $a \in I$, write

$$a = \sum_{j \in J(a)} a_j \otimes d_j$$

Since I is a two-sided ideal we have for any nonzero $d \in D$ and $j_0 \in J(a)$,

$$ad = \sum_{j \in J(a)} (d_j d) \cdot (a_j \otimes 1) \in I$$

$$\implies J(a - (d_{j_0} d^{-1} d_{j_0}^{-1}) \cdot (ad)) = J \left(\sum_{j \in J(a)} (d_j - d_{j_0} d^{-1} d_{j_0}^{-1} d_j d) \cdot (a_j \otimes 1) \right) \subseteq J(a) \setminus \{j_0\}$$

and so by the minimality assumption of a being primordial $a = (d_{j_0} d^{-1} d_{j_0}^{-1}) \cdot (ad)$. Since we assumed $d_{j_0} = 1$ for some j_0, that implies $a = d^{-1} \cdot (ad)$. Writing in the basis,

$$0 = \sum_{j \in J(a)} a_j \otimes (d_j - d^{-1} d_j d) \implies d_j d = d d_j \ \forall j$$

Since d was arbitrary and D was central, that means each d_j is in k, i.e. $a \in A \otimes 1$. But now, since I was a two-sided ideal and A was simple we can generate all of $A \otimes 1$ by acting on a by elements of the form $a \otimes 1$, and get all of $A \otimes_k D$ via elements $1 \otimes d$. Thus, $I = A \otimes_k D$, which is simple. ∎

The final ingredient in the construction of the Brauer group is the introduction of an equivalence relation that ensures every central simples algebra (abbreviated **CSA**) is invertible under the tensor product. In particular, central simple k-algebras A and B are defined to be **similar**, written $A \sim B$, if $A \otimes_k M_n(k) \cong B \otimes_k M_m(k)$ for some $m, n \in \mathbb{N}$.

Lemma 1.4

Under $\otimes_k$, the equivalence classes of CSAs under similarity forms an abelian group.

Proof. Since the tensor product is commutative and associative with identity element k, it suffices to show that it respects similarity classes and that every CSA has an inverse. The former is true because

$$A \otimes M_n(k) \cong A' \otimes M_{n'}(k), B \otimes M_m(k) \cong B' \otimes M_{m'}(k) \implies$$

$$(A \otimes B) \otimes M_{nm}(k) \cong (A' \otimes B') \otimes M_{n'm'}(k)$$

For a CSA A recall that A^{opp} was given by the same elements as A but multiplication reversed. Define a map $\Phi : A \otimes_k A^{\text{opp}} \to \text{End}_k(A)$ by $a \otimes a' \mapsto (v \mapsto ava')$. The image of $a \otimes a'$ is k-linear because $\lambda v \mapsto a(kv)a' = \lambda(ava')$. Moreover, Φ is well-defined and k-linear by a similar calculation, and a ring homomorphism because

$$\Phi(a \otimes a')\Phi(b \otimes b')v = abvb'a' = (ab)v(a' \times_{\text{opp}} b') = \Phi\left((a \otimes a')(b \otimes b')\right) v$$

We've already shown that $A \otimes_k A^{\text{opp}}$ is simple, and so the kernel of Φ must be 0 (since it doesn't contain 1). Moreover, $A \otimes_k A^{\text{opp}}$ and $\text{End}_k(A)$ both have dimension $\dim(A)^2$ over k. Thus, $A \otimes_k A^{\text{opp}} \cong \text{End}_k(A) \cong M_n(k)$, which is the identity class in $\text{Br}(k)$. $\square$

Note that because $M_n(D) = D \otimes_k M_n(k)$, when calculating the elements of the Brauer group it suffices to merely find all central division algebras. Any two distinct division algebras will give distinct elements of the Brauer group because $M_n(D) \otimes M_m(k) = M_{nm}(D)$ and we showed how to recover D (as the centralizer of $M_{nm}(D)$) from the matrix algebra.

Example 1.5

We can say something about the Brauer group of all of the fields we care about in number theory:

- First, let's look at the Brauer groups of the Archimedean local fields. It's a standard result due to Frobenius that the real associative division algebras are $\mathbb{R}, \mathbb{C}, \mathbb{H}$. Both $\mathbb{R}$ and $\mathbb{C}$ are fields and the center of the quaternions $\mathbb{H}$ is $\mathbb{R}$. Thus there are two equivalence classes of CSAs over $\mathbb{R}$ and the Brauer group of $\mathbb{C}$ is trivial. The complex case easily generalizes to any algebraically closed field: if D is a division algebra over k then for any nonzero element α, $k[\alpha]$ is a finite field extension of k (a field since it's a k-finite-dimensional integral domain) and thus equal to k, meaning $D = k$.

- We'll show in the next section that the Brauer group of a finite field is trivial.

- In the next section we'll discuss how to see that the Brauer group of a nonarchimedean local field is $\mathbb{Q}/\mathbb{Z}$. The global case is more difficult and omitted, but it is true that for an arbitrary number field K there is an exact sequence

$$0 \to \mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \xrightarrow{\sum} \mathbb{Q}/\mathbb{Z} \to 0$$

  where the direct sum is taken over places of K, the map to $\mathbb{Q}/\mathbb{Z}$ is given by the sum of the maps we will construct in the next section, and the map $\mathrm{Br}(K) \to \mathrm{Br}(K_v)$ is from the embedding $K \to K_v$ as described below.

For $k \subseteq L$ arbitrary fields (with L not necessarily finite degree over k), there's a map $\mathrm{Br}(k) \to \mathrm{Br}(L)$ given by $A \mapsto A \otimes_k L$. The image is an algebra over L by acting on the second factor, it is central because $Z(A \otimes_k L) = Z(A) \otimes_k Z(L) = k \otimes_k L = L$, and it is simple because the tensor product of simple k-algebras with one of them k-central is simple. Furthermore, this map is a group homomorphism because by the associativity of tensor products (over not necessarily equal rings) and commutativity,

$$(A_1 \otimes_k L) \otimes_L (A_2 \otimes_k L) \cong A_1 \otimes_k (L \otimes_L (L \otimes_k A_2)) \cong A_1 \otimes_k ((L \otimes_L L) \otimes_k A_2) \cong (A_1 \otimes_k A_2) \otimes_k L$$

The kernel of this map, i.e. the A such that $A \otimes_k L$ is a matrix algebra over L, is called the **relative Brauer group $\mathrm{Br}(L/k)$**, and it is this group which can be shown to be naturally isomorphic to $H^2(L/k)$. We say that elements of $\mathrm{Br}(L/k) \subset \mathrm{Br}(k)$ are **split by L**.

§2 The Brauer Group of a Nonarchimedean Local Field

The goal of this section will be the following theorem

Theorem 2.1

For K a nonarchimedean local field, $\mathrm{Br}(K) \equiv \mathbb{Q}/\mathbb{Z}$.

The majority of the exposition will be devoted to the construction of the isomorphism, and then with the remaining space I will try to give an idea for why it is bijective and relate it to cohomology.

§2.1 Construction of $\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$

Let D be an arbitrary central division algebra over K. The first thing we can do is extend the usual structures on K coming from the valuation to D. For any $\alpha \in K$ the subalgebra $K[\alpha]$ is a finite-dimensional integral domain, and so it is a field extension of K. By completeness of K, $|\cdot|_K$ extends uniquely to $K[\alpha]$, giving a unique extension to all of D. Using this absolute value, we can extend the valuation on K by the same formula, $|\alpha| = q^{-v(\alpha)}$ where q is the size of the residue field k of K. Furthermore, we can make similar ring of integers definitions as for the local field with

$$\mathcal{O}_D := \{d \in D : v(d) \geq 0\} \text{ and } \mathfrak{P} := \{d \in D : v(d) > 0\}$$

To show that these satisfies the expected algebraic properties, we need to show that the extension of $|\cdot|_K$ to D is in fact an absolute value, i.e.

$$|\alpha\beta| = |\alpha\beta| \qquad |\alpha + \beta| \leq \max\{|\alpha|, |\beta|\} \qquad |\alpha| \geq 0, \text{ and } = 0 \text{ iff } \alpha = 0$$

The third property here is immediate from the definition, but the other two are nontrivial seeing as how α, β need not be contained in a subfield. The method to prove them is not mentioned in Milne's exposition, but there are several ways (each unfortunately involved enough to be omitted here): in the first chapter of [4] the absolute value $|x|$ is constructed as the scaling factor multiplication by x acts on the additive Haar measure of D (by uniqueness of the Haar measure) which can be shown to satisfy these algebraic properties and agree with the absolute value on subfields; alternatively in the second and third chapters of [3] they are proved by constructing the "reduced norm" defined by $\det(d \otimes 1)$ where $d \otimes 1 \in D \otimes_K L$ for an L splitting D (recall this means $D \otimes_K L = M_n(L)$).

With these properties, $\mathcal{O}_D$ is a subring of D which agrees with the standard ring of integers on any subfield of L, i.e. $\mathcal{O}_D$ is precisely the elements of D which are integral over $\mathcal{O}_K$. Since the valuation is a homomorphism, $\mathfrak{P}$ is similarly a two-sided ideal of $\mathcal{O}_D$. Any nonzero element of $\mathcal{O}_D \setminus \mathfrak{P}$ must be a unit because $|d| = 1 \implies |d^{-1}| = 1$ by mutliplicativity of the absolute value, so $\mathcal{O}_D$ is a maximal two-sided ideal, and in fact any two-sided ideal is a power of $\mathfrak{P}$ (again by restricting to subfields).

To further investigate the structure of $\mathcal{O}_D$, we will need the "Noether-Skolem Theorem" several times.

Theorem 2.2 (Noether-Skolem)

For $f, g : A \to B$ maps of K algebras (K any field) such that A is simple and B is a CSA, there exists $b \in B$ invertible such that $f(a) = bg(a)b^{-1}$ for all $a \in A$.

Proof. From f, g, we obtain maps $f \otimes 1, g \otimes 1 : A \otimes_K B^{\mathrm{opp}} \to B \otimes_K B^{\mathrm{opp}} \cong M_n(K)$. First, we'll produce an invertible $b_0 \in B \otimes_K B^{\mathrm{opp}} \cong M_n(K)$ such that

$$(f \otimes 1)(a \otimes b) = b_0(g \otimes 1)(a \otimes b)b_0^{-1}$$

for all $a \in A, b \in B^{\mathrm{opp}}$. Fixing an isomorphism $B \otimes_K B^{\mathrm{opp}} \cong M_n(K)$, it suffices to find an A-module isomorphism between $(K^n, a \mapsto (f \otimes 1)(a \otimes 1))$ and $(K^n, a \mapsto (g \otimes 1)(a \otimes 1))$ because that's the same as an invertible element of $b_0 \in M_n(K)$ with (for all $v \in K^n = B$)

$$b_0^{-1}(f \otimes 1)(a \otimes 1)v = (g \otimes 1)(a \otimes 1)b_0^{-1}v \implies f(a)vb = (b_0 g(a)(b_0^{-1}v))b$$

$$\iff (f \otimes 1)(a \otimes b)v = b_0(g \otimes 1)(a \otimes b)b_0^{-1}v$$

Such an A-module isomorphism exists because of the fact that modules over a simple algebra of the same k-dimension are necessarily isomorphic, which we will now prove. It is in fact true that every (finitely-generated) module over $A \cong M_m(D)$ is isomorphic to the direct sum of some number of copies of the standard module D^m. Since a finitely-generated module is a quotient of copies of A and quotients of semi-simple modules are semisimple, we know every A-module is semisimple if A is itself as an A-module. This is true: $M_m(D) \cong D^m \oplus \cdots \oplus D^m$ m times where the ith copy of D^m is the matrices which are nonzero in only the ith column (note that D^m is simple because permutation matrices bring any element of the standard basis to any other). To complete this part of the proof then, it suffices to show that all simple A-modules are isomorphic. Every simple A-module M is a quotient of A because of the surjective A-module map $a \mapsto am$ for nonzero $m \in M$. But we already discussed how A decomposes into m copies of the same simple A-module D^m, and this decomposition is unique up to permutation by the standard Jordan-Hölder argument for A-modules.

Having produced the desired b_0, we have that for all $b \in B$

$$(f \otimes 1)(a \otimes b) = b_0(g \otimes 1)(a \otimes b)b_0^{-1} \underset{a=1}{\Longrightarrow} 1 \otimes b = b_0(1 \otimes b)b_0^{-1} \implies b_0 \in C(k \otimes B^{\text{opp}})$$

i.e. b_0 commutes with $k \otimes B^{\text{opp}}$ in $B \otimes B^{\text{opp}}$. The argument we gave at the beginning of our Lemma 1.3 extends directly to show that the centralizer of the tensor product of subalgebras is the tensor product of the given centralizers, so by the assumption that B is central we have that $b_0 = b_0' \otimes 1 \in B \otimes k \subset B \otimes B^{\text{opp}}$. In particular,

$$(f \otimes 1)(a \otimes b) = (b_0' \otimes 1)(g \otimes 1)(a \otimes b)(b_0'^{-1} \otimes 1) \implies$$

$$f(a) \otimes 1 = b_0' g(a) b_0'^{-1} \otimes 1 \implies f(a) = b_0' g(a) b_0'^{-1}$$

□

Now, an immediate restriction on dimensions is the following:

Lemma 2.3

For CSA A over arbitrary field K, $[A : K]$ must be a square. The maximal subfields of a central simple K-division algebra D containing K are exactly those of degree $\sqrt{[D : K]}$.

Proof. Choosing a separable closure $K \to K^{\text{sep}}$, any CSA A must satisfy $[A : K] = [A \otimes_K K^{\text{sep}} : K^{\text{sep}}]$ by usual extension of scalars. By acting on the second factor $A \otimes_K K^{\text{sep}}$ becomes a simple K^{sep}-algebra, and by the example from the last section the only division algebra over K^{sep} is K^{sep} itself. Thus, $A \otimes_K K^{\text{sep}} \cong M_n(K^{\text{sep}})$ for some n, which has dimension n^2.

Now, subfields L containing K are exactly K-subalgebras (again because D is finite-dimensional over K). If L is maximal in this sense then the centralizer of L in A (as elements of A) is exactly L because if $a \in C(L) \setminus L$ then $L[a]$ would be a field containing L. The rest of the proof will be dedicated to the fact that if B is a simple K-subalgebra of a K-CSA A then the centralizer (as elements of A) $C = C(B)$ is simple, $C(C(B)) = B$, and

$$[B : K] \cdot [C : K] = [A : K]$$

This will complete the proof because then for maximal L we have

$$[L : K][C(L) : K] = [L : K]^2 = [A : K]$$

and conversely if $[L:K]^2 = [A:K]$ then any maximal L' containing L would satisfy the same and so $[L:K] = [L':K] \implies L = L'$ is maximal.

So, we prove the above statement for arbitrary A, B. Since CSAs are closed under tensor product, $A \otimes_K \operatorname{End}_K(B)$ is central simple. As discussed previously, centralizers respect tensor products so inside $A \otimes_K \operatorname{End}_K(B)$ the centralizer of $B \otimes 1$ is $C(B) \otimes_K \operatorname{End}_K(B) = C \otimes_K \operatorname{End}_K(B)$ and the centralizer of $1 \otimes_K B$ is $A \otimes_K C_{\operatorname{End}_K(B)}(B)$. To calculate this second expression, observe that a K-linear map commuting with B is precisely a B-linear map, which is determined by where it sends 1, so the centralizer of $1 \otimes_K B$ is $A \otimes_K B^{\text{opp}}$ (multiplication is reversed because $\phi(b) = \phi(b \cdot 1) = b\phi(1)$ means that B-linear maps act by right multiplication instead of left). Applying the Noether-Skolem Theorem to $f, g : B \to A \otimes_K \operatorname{End}_K(B)$ by $f : b \mapsto b \otimes 1, g : b \mapsto 1 \otimes b$ we obtain invertible $u \in A \otimes_K \operatorname{End}_K(B)$ with

$$b \otimes 1 = u(1 \otimes b)u^{-1}, \forall b \in B \implies C_{A \otimes_K \operatorname{End}_K(B)}(B \otimes 1) = u \cdot C_{A \otimes_K \operatorname{End}_K(B)}(1 \otimes B) \cdot u^{-1}$$

$$\implies C \otimes_K \operatorname{End}_K(B) = u(A \otimes_K B^{\text{opp}})u^{-1} \implies C \otimes_K \operatorname{End}_K(B) \cong A \otimes_K B^{\text{opp}}$$

By our Lemma 1.3 $A \otimes_K B^{\text{opp}}$ is simple, so $C \otimes_K \operatorname{End}_K(B)$ is. Clearly if I is an ideal of C then $I \otimes_K \operatorname{End}_K(B)$ would be an ideal, so in fact C is simple. Moreover, the isomorphism above gives the degree calculation:

$$[C:K] \cdot [B:K]^2 = [A:K] \cdot [B:K] \implies [C:K] \cdot [B:K] = [A:K]$$

Finally, $B \subset C(C(B))$ by definition and because $C(B)$ itself is simple we have by this last formula that $[C(C(B)):K] \cdot [C:K] = [A:K]$ and so $[B:K] = [C(C(B)):K]$, giving equality. □

With this lemma in hand, write $n^2 = [D:K]$. For any subfield L containing K recall that a way to construct the extension of an absolute value on L is $|\ell| = |N_K^L(\ell)|^{1/[L:K]}$. Since we've normalized as usual on K such that $v(K^\times) = \mathbb{Z}$, extending $K[d]$ to a maximal such field L we have that $[L:K] = n$ and so $v(D^\times) \subset \frac{1}{n}\mathbb{Z}$. Writing the two-sided ideal generated by $\mathfrak{p}$ in $\mathcal{O}_D$ as $\mathfrak{P}^e$ by our earlier work, $v(D^\times) = \frac{1}{e}\mathbb{Z} \subset \frac{1}{n}\mathbb{Z}$, and so $e|n$.

We can also consider the analogue of the residue field: define $d := \mathcal{O}_D/\mathfrak{P}$. This d must be a division algebra because as discussed the elements of $\mathcal{O}_D \setminus \mathfrak{P}$ are units, so certainly every element of the quotient is invertible. Seeing as d is a finite-dimensional division algebra over the finite residue field k, the following lemma will tell us that in fact d is a field; denote by f its degree d/k as usual (note that following lemma doesn't guarantee $d = k$ because we don't know that d is central over k; the center could be larger).

Lemma 2.4

The Brauer group of a finite field is trivial. In particular, every division algebra with finitely-many elements is a field.

Proof. Let D be a division algebra with a finite number of elements and center k'. By the previous lemma, $[D:k'] = m^2$ is a square, and every element $d \in D$ is contained in $k'[d] \subset \ell$ a maximal subfield of cardinality $|k'|^n$. By the uniqueness of finite fields, each of these ℓ is isomorphic. Letting $\phi : \ell_1 \to \ell_2$ be such an isomorphism, we can define maps $f, g : \ell_1 \to D$ by $f = \text{id}, g = \phi$ and use Noether-Skolem to obtain $\alpha = \beta\phi(\alpha)\beta^{-1}$ for any $\alpha \in \ell_1$ and a fixed $\beta \in D$, i.e. $\ell_1 = \beta\ell_2\beta^{-1}$. Letting ℓ_2 vary, we have

$$D^\times = \bigcup_{\beta \in D^\times} \beta\ell_1^\times\beta^{-1} \implies D^\times = \ell_1^\times$$

because the number of distinct conjugates of $\ell_1^\times$ could be at most $\frac{|D^\times|}{|\ell^\times|}$, but the identity is contained in each so the union could only cover all of $D^\times$ if $D = \ell_1$. Since D is therefore commutative, $D = k'$. ☐

With $d = \mathcal{O}_D/\mathfrak{P}$ being degree f over the residue field k, write $d = k[a]$ by the primitive element theorem. Lifting a to any $\alpha \in \mathcal{O}_D$, the fact that $[K[\alpha] : K] \leq n$ implies $[k[a] : k] = f \leq n$.

Now having that $e, f \leq n$, once we show that $n^2 = [D : K] = ef$ as in the standard setup, we will have that $e = f = n$. The proof of that fact follows some a similar path as for ordinary extensions of fields. First, note that because K is a local field, $\mathcal{O}_K$ is a DVR and thus a PID, so we know that $\mathcal{O}_D$ is a free $\mathcal{O}_K$-module once we've shown that it is finitely-generated and torsion-free as a module (this follows from the classification of finitely-generated modules over a PID). The fact that $\mathcal{O}_D$ is torsion-free is immediate because D is a division algebra. For the finitely-generated portion I'll return to the proof given in Lang's algebraic number theory for extensions of fields. Take basis $\{d_1, \dots, d_{n^2}\}$ for D over K. Since D is K-finite dimensional we know any d is integral over K so since K is just the field of fractions of $\mathcal{O}_K$ we can multiply through by denominators to make each element of this basis integral over $\mathcal{O}_K$. Now, the trace map $(d_1, d_2) \mapsto \mathrm{Tr}_K^D(d_1 \cdot d_2)$ is still K-bilinear and must be non-degenerate because if d were in the kernel then the trace map on the field $K[d]$ would be degenerate. Therefore, letting $\{d_1', \dots, d_{n^2}'\}$ be a dual basis to $\{d_i\}$ under the trace map, finitely-generated follows (as in the field extension case, since $\mathcal{O}_K$ is Noetherian) by showing

$$\mathcal{O}_K d_1 + \cdots + \mathcal{O}_K d_{n^2} \subset \mathcal{O}_D \subset \mathcal{O}_K d_1' + \cdots + \mathcal{O}_K d_{n^2}'$$

The first inclusion was by construction and the second is because if we write $b = \sum_i k_i d_i'$ then

$$\mathrm{Tr}(b \cdot d_j) = \sum_i k_i \,\mathrm{Tr}(d_i' d_i) = k_j$$

and since $\mathcal{O}_D$ is a subring we know $b \cdot d_j \in \mathcal{O}_D$ and furthermore since these elements still have minimal polynomials with coefficients in $\mathcal{O}_K$, we know that this trace is in $\mathcal{O}_K$.

Knowing that $\mathcal{O}_D$ is a finite-dimensional free $\mathcal{O}_K$-module, its rank can be determined because $\mathcal{O}_D \otimes_{\mathcal{O}_K} K = D$ by the same clearing of denominators we did for the basis $\{d_i\}$ above, so the rank is just the dimension $[D : K] = n^2$. Moreover,

$$\mathcal{O}_D \otimes_{\mathcal{O}_K} k = \mathcal{O}_D \otimes_{\mathcal{O}_K} (\mathcal{O}_K/\mathfrak{p}) \cong \mathcal{O}_D/\mathfrak{p}\mathcal{O}_D = \mathcal{O}_D/\mathfrak{P}^e$$

using the standard isomorphism $d \otimes [\alpha] \mapsto [\alpha]d$ (with inverse $[d] \mapsto d \otimes 1$). In particular, since $\mathcal{O}_K \otimes_{\mathcal{O}_K} k = k$, this implies that $\mathcal{O}_D/\mathfrak{P}^e$ has dimension n^2 over k. However, recall that $d = \mathcal{O}_D/\mathfrak{P}$ had dimension f over k and

$$\mathcal{O}_D \supset \mathfrak{P} \supset \mathfrak{P}^2 \supset \cdots \supset \mathfrak{P}^e$$

where each $\mathfrak{P}^i/\mathfrak{P}^{i+1}$ is a d-vector space and must have dimension 1 because otherwise there would be an ideal between $\mathfrak{P}^i$ and $\mathfrak{P}^{i+1}$. Thus,

$$n^2 = [\mathcal{O}_D/\mathfrak{P}^e : k] = [\mathcal{O}_D/\mathfrak{P}^e : d] \cdot [d : k] = ef \implies n = e = f$$

With this understanding of the structure of D, we are finally prepared to define the map $\mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$, denoted $D \mapsto \mathrm{inv}_K(D)$. Using the primitive element theorem, again write $d = \mathcal{O}_D/\mathfrak{P} = k[a]$ and let $\alpha \in \mathcal{O}_D$ be a lift of a. Then $\mathcal{O}_{K[\alpha]}/(\mathfrak{P} \cap \mathcal{O}_{K[\alpha]}) = k[a] = d$, so by the usual "$ef = n$" formula for local fields, $[K[\alpha] : K] \geq [d : k] = n$. However, we've already showed that maximal subfields of D containing K are precisely those of degree n, so $[K[\alpha] : K] = n$ and the ramification index is 1. In particular, for each central division algebra D we've constructed a maximal subfield $L = K[\alpha]$ containing K which is unramified over K.

Now, recall that for an unramified extension L of a local field there is a unique Frobenius automorphism σ lifting the Frobenius automorphism of the residue field (shown for instance in the first chapter of [4]). Now, we can define maps $f, g : L \to D$ by $f = \sigma$ and g is just inclusion, which are maps of K-algebras. By Noether-Skolem, there exists some $d \in D$ with $\sigma(x) = dxd^{-1}$ for all $x \in L$. If $c \in L^\times$ is arbitrary then we have

$$(cd)x(cd)^{-1} = c(dxd^{-1})c^{-1} = c\sigma(x)c^{-1} = \sigma(x)$$

and conversely suppose that $\sigma(x) = d'x(d')^{-1}$. Then

$$d'x(d')^{-1} = dxd^{-1} \implies d^{-1}d'x = xd^{-1}d' \implies d^{-1}d' \in C(L) = L$$

where we are using maximality of L to give (as in our Lemma 2.3) that $[L : K][C(L) : K] = n[C(L) : K] = n^2$ means that $[C(L) : K] = n$ and so must be exactly $C(L) = L$. In particular, $d' = cl$ for some $c \in L$, so this conjugation element is uniquely determined up to left-multiplication by elements of L. Thus, we can define the map $\text{inv}_K = D \mapsto v(d) \in \mathbb{Q}/\mathbb{Z}$ defined in terms of the Frobenius automorphism because

$$v(d') = v(c) + v(d) \equiv v(d) \bmod \mathbb{Z}$$

§2.2 Bijectivity of inv_K and Relation to Cohomology

I'll now attempt to give a sketch of why this map is bijective, relying on some facts about cohomology. Recall that this subfield L we constructed is actually unique up to isomorphism: we showed in Theorem 2.6 of our class notes "Extensions of Complete Fields" that the functor sending unramified extensions of K to finite extensions of k is an equivalence of categories, and so the degree-n unramified extension L of K is unique up to isomorphism by the classification of finite fields. Fixing an algebraic closure $\overline{K}$ of K, we can view each such L as a subfield of $\overline{K}$ and denote the residue extensions by l/k.

First, note that the norm maps $l \to k, l^\times \to k^\times$ are surjective. This can be shown directly as follows. Let $|k| = p^m = q, [l : k] = n$, and let α be a generator for $l^\times$ (which we've shown previously is cyclic), meaning $N_k^l(\alpha) = \alpha \cdot \alpha^q \cdots \alpha^{q^{n-1}}$ since the Galois group is generated by the qth-power map. However, the fact that α generates $l^\times$ means the order of α is $q^n - 1$. Since $q^n - 1 = (q-1)(1 + \cdots + q^{n-1})$, that means the order of $N_k^l(\alpha)$ is $q - 1$, so it generates all of $k^\times$. Now, recall that in one of the homework assignments we worked with the principal unit and higher unit groups $U^{(i)} = 1 + \mathfrak{p}^i$, descending neighborhoods of 1 (constructed in both L and K). Because $U^{(i)}/U^{(i+1)} = \mathcal{O}/\mathfrak{p}$ and the norm maps are surjective (and behaves nicely with these neighborhoods), $U_L \to U_K$ is surjective (see page 122 of Neukirch [2] for details).

Now, we will need to use results about cohomology. The purpose of the last paragraph was to obtain that $H_T^0(G, U_L) = 0$ for $G = \text{Gal}(L/K)$. We discussed in class that this zeroth Tate cohomology can be constructed as $U_L^G/N(U_L)$, which in this case is $U_K/U_K = 0$ by surjectivity of the norm. Since G is cyclic, $H^2(G, U_L) = H_T^0(G, U_L)$ (see [1] page 81, Proposition 3.4), so it is also trivial. Writing in terms of a uniformizer $L^\times = U_L \times \pi^{\mathbb{Z}}$,

$$\text{Br}(L/K) \cong H^2(L/K) = H^2(G, L^\times) = H^2(G, U_L) \times H^2(G, \pi^{\mathbb{Z}}) = H^2(G, \pi^{\mathbb{Z}})$$

(cohomology respects products by Proposition 1.25 on page 68 of [1]). This cohomology $H^2(G, \pi^{\mathbb{Z}})$ is easier to calculate as cyclic of order $n = [L : K]$ (page 102 of [1]), and more explicitly we can write down the cocycle φ generating it: if $G = \langle \sigma \rangle$,

$$\varphi(\sigma^i, \sigma^j) = \begin{cases} 1, i + j \leq n - 1 \\ \pi, i + j > n + 1 \end{cases}$$

Under the isomorphism $\mathrm{Br}(L/K) \cong H^2(L/K)$, the CSA $A(\varphi)$ we recover from φ satisfies $\mathrm{inv}_K(A(\varphi)) = \frac{1}{n}$, and so using that each element of $\mathrm{Br}(K)$ is in $\mathrm{Br}(L)$ for some L, the map inv_K is a bijection with inverse given by the preceding construction.

To conclude, I will prove the fact that each element of $\mathrm{Br}(K)$ is in $\mathrm{Br}(L)$ for some L. The construction of a CSA from a cocycle is also reasonably attainable, but unfortunately I am already out of space to include it.

Lemma 2.5

For L finite Galois subextensions of K inside $\overline{K}$,

$$\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L/K)$$

Proof. First note that maximal subfields of a central division algebra D necessarily split D because as in our Lemma 2.3, that means $L = C(L)$ in D and so

$$\mathrm{End}_L(D) = C_{D \otimes_K D^{\mathrm{opp}}}(1 \otimes L) = D \otimes_K L$$

which is a matrix ring over L. By possibly passing to the Galois closure of L (larger fields still split, because the tensor product is then just change of scalars of matrices), it therefore suffices to show that every D contains a maximal separable extension of K. Taking L to be a maximal subfield of D among those which are separable, suppose for the sake of contradiction L is not maximal as a subfield containing K. By the degree calculation in our Lemma 2.3, that implies $C(L)$ is an L-central division algebra strictly bigger than L. Therefore, to contradict our maximality assumption it suffices to show that every central division algebra which is not a field contains a subfield separable over its center, but strictly bigger than the center.

So, return to D being a central division algebra over K. Since the desired statement is trivial for K perfect, assume K has characteristic $p \neq 0$ and is infinite. Let $\{d_i\}$ be a basis for D over K with $d_1 = 1$ and structure constants $d_i d_j = \sum_l c_{i,j,l} d_l$. Suppose for the sake of contradiction that $K[a]$ is purely inseparable over K for all $a \in D$, i.e. there is a positive integer k with $a^{p^r} \in K$ (and by finite-dimensionality this r can be taken globally for all of D). Now, write $P_i(m, a_1, \ldots, a_{n^2})$ for the polynomial in the $a_j \in K$ (depending only on the structure constants) defined by

$$\left(\sum_i a_i d_i \right)^m = \sum_i P_i(m, a_1, \ldots, a_{n^2}) d_i$$

Clearly for all $i \neq 1$ and any a_j we have $P_i(p^r, a_1, \ldots, a_{n^2}) = 0$ and so $P_i(p^r, X_1, \ldots, X_{n^2})$ is the zero polynomial (for any infinite field, a polynomial is zero iff it gives rise to the zero function). However, for $a \in D \otimes_K K^{\mathrm{alg}}$,

$$a = \sum_i a_i (d_i \otimes 1), a_i \in K^{\mathrm{alg}} \implies a^m = \sum_i P_i(m, a_1, \ldots, a_{n^2}) d_i \otimes 1$$

so $a^{p^r} \in K^{\text{alg}}$. As in Lemma 2.3, $D \otimes_K K^{\text{alg}} = M_n(K^{\text{alg}})$ and so if $n \neq 1$ (i.e. if D were not a field) the matrix C with 1 in the top left entry and zero everywhere else would satisfy $C^{p^r} \in K^{\text{alg}} I_{n\times n}$ even though $C^{p^r} = C \notin K^{\text{alg}} I_{n\times n}$. $\square$

References

[1] Milne, J.S. (2020). *Class Field Theory.* https://www.jmilne.org/math/CourseNotes/CFT.pdf.

[2] Neukirch, Jrgen (199). *Algebraic Number Theory.*

[3] Reiner, Irving (1973). *Maximal Orders.*

[4] Weil, Andr (1995). *Basic Number Theory.* https://link.springer.com/book/10.1007/978-3-642-61945-8.