Brauer groups and Galois Cohomology

1 Introduction

The main goal of the next talks is to prove the following theorem:

Theorem 1.1. *Let K be a field extension of transcendence degree 1 over an algebraically closed field k. Then $H^2_{ét}(\operatorname{Spec} K, \mathbb{G}_m) = 0$.*

Let k be an arbitrary field, and fix a separable closure k^{sep} of k, and let $G_k := \operatorname{Gal}(k^{\text{sep}}/k)$. The first step is to show

Theorem 1.2 (Corollary 4.10)**.** *There is a natural bijection*

$$H^2\big(G_k, (k^{\text{sep}})^\times\big) \cong \operatorname{Br}(k), \tag{1.1}$$

where $\operatorname{Br}(k)$ is the Brauer group of k.

This is aim of the current talk. The main references are [1, Chapter IV] and [2, Tag 073W].

2 Central simple algebras

2.1 Basic definitions and properties

Let k be a field. In what follows, we use the term *k-algebra* to refer to an associative unital k-algebra which is **finite dimensional** as a k-vector space. In particular, we do **not** assume that k-algebras are commutative.

Definition 2.1. *A k-algebra is called* simple *if it contains no proper two sided ideals other than* (0).

Definition 2.2. *A k-algebra A is said to be* central *if its center $Z(A)$ is equal to k. If A is also simple, we say that it is* central simple.

We say a k-algebra D is a *division algebra* if every non-zero element has a multiplicative inverse, i.e., for every $a \in D \setminus \{0\}$, there exists a $b \in D$ such that $ab = 1 = ba$. A *field* is a commutative division algebra.

Proposition 2.3. *Let D be a division algebra over k. Then $M_n(D)$ is a simple k-algebra for all $n \geqslant 0$.*

Proof. Let I be a two-sided ideal in $M_n(D)$ and suppose that I contains a nonzero matrix $M = (m_{ij})$. Let $m_{i_0 j_0}$ be a non-zero entry of M. For each i, j, let $e_{ij} \in M_n(D)$ denote the matrix with 1 in the ij-entry and 0 elsewhere. Then

$$e_{ii_0} \cdot M \cdot e_{j_0 j} = m_{i_0 j_0} e_{ij}.$$

By assumption, the left hand side is in I, so I contains all the matrices e_{ij} and thus equals $M_n(D)$. It follows that $M_n(D)$ is simple. □

2.2 Classification of simple k-algebras

Let A be a k-algebra. By an A-*module*, we mean a finitely generated **left** A-module. A non-zero A-module is called *simple* if it contains no proper A-submodule.

Lemma 2.4. *Any non-zero A-module contains a simple submodule.*

Proof. The definition implies that any A-module is finite dimensional as a k-vector space. Any nonzero submodule of minimal dimension over k will be simple. □

Let V be an A-module. Then $\operatorname{End}_A(V)$ inherits the structure of a k-algebra, with multiplication given by composition.

Lemma 2.5 (Schur's Lemma)**.** *Let S be a simple A-module. The k-algebra $\operatorname{End}_A(S)$ is a division algebra.*

Proof. Let $\gamma \in \operatorname{End}_A(S)$. Then $\ker \gamma$ is an A-submodule of S and is thus either 0 or all of S. In the first case γ is an isomorphism and thus has an inverse. Otherwise $\gamma = 0$. □

There is a natural homomorphism

$$\ell \colon A \to \operatorname{End}_k(V), \quad a \mapsto \ell_a, \tag{2.1}$$

where ℓ_a is left multiplication by a.

Proposition 2.6. *Let A be a simple k-algebra and let V be an A-module. The homomorphism (2.1) is injective.*

Proof. Since $\ker(\ell)$ is a two-sided ideal of A which does not contain 1, it follows from the simplicity of A that $\ker(\ell) = (0)$. □

When A is simple, we may thus view it as a k-subalgebra of $\operatorname{End}_k(V)$. Suppose A is a k-subalgebra of another k-algebra B. We denote the *centralizer* of A in B by $C_B(A)$.

Theorem 2.7 (Double Centralizer Theorem)**.** *Let A be a simple k-algebra, and let S be a simple A-module. Let $E := \operatorname{End}_k(S)$. We have $C_E\big(C_E(A)\big) = A$.*

Proof. See [1, Theorem 1.13]. □

Definition 2.8. *Given a k-algebra A, we define its* opposite A^{opp} *to be the algebra with the same underlying set and addition, but with multiplication defined by $a \cdot b := ba$.*

Proposition 2.9. *Let A be a k-algebra and let V be a free A-module of rank n. Then any choice of basis of V induces an isomorphism of k-algebras $\mathrm{End}_A(V) \xrightarrow{\sim} M_n(A^{\mathrm{opp}})$.*

Proof. Let ${}_AA$ denote A regarded as an A-module. For each $a \in A$, right multiplication by a is an A-linear endomorphism of ${}_AA$. Let $r_a \in \mathrm{End}_A({}_AA)$ denote this endomorphism. Let $\varphi \in \mathrm{End}_A({}_AA)$. For $a \in {}_AA$, we have $\varphi(a) = a\varphi(1)$ by A-linearity; hence $\varphi = r_{\varphi(1)}$. We thus have an isomorphism **of k-vector spaces**

$$\mathrm{End}_A({}_AA) \xrightarrow{\sim} A, \quad \varphi \mapsto \varphi(1). \tag{2.2}$$

Since

$$(r_a \circ r_b)(1) = r_a\big(r_b(1)\big) = r_a(b) = ba,$$

the k-linear map (2.2) becomes an isomorphism $\mathrm{End}_A({}_AA) \xrightarrow{\sim} A^{\mathrm{opp}}$ on the level of k-algebras. This implies the lemma since any choice of A-basis of V induces an isomorphism of k-algebras $\mathrm{End}_A(V) \xrightarrow{\sim} \mathrm{End}_A({}_AA^n)$. □

In the next theorem, we classify all simple k-algebras up to isomorphism.

Theorem 2.10 (Artin-Wedderburn)**.** *Let A be a simple k-algebra. Then there exists an $n \geqslant 1$ and a division algebra D such that $A \cong M_n(D)$.*

Proof. By Lemma 2.4, we may choose a simple A-submodule $I \subset A$ (a left ideal of minimal dimension). By Schur's Lemma, the k-algebra $D := \mathrm{End}_A(I)$ is a division algebra. Since $\dim_k(I) < \infty$, it follows that I is finitely generated over D. It is thus a free D-module of some finite rank n.[1] Let $E := \mathrm{End}_k(S)$. Since $D = C_E(A)$, we have

$$\mathrm{End}_D(I) = C_E(D) = C_E\big(C_E(A)\big) = A;$$

hence $A \cong M_n(D^{\mathrm{opp}})$ by Proposition 2.9. □

Proposition 2.11. *In Theorem 2.10, the k-algebra A uniquely determines is isomorphism class of D and the integer n.*

Proof. The minimal left ideals of $M_n(D)$ are of the form $L(i)$, where $L(i)$ is the set of matrices that are 0 outside of the ith column. Then $M_n(D) = \oplus_{i=1}^n L(i)$ and each $L(i) \cong D^n$ as $M_n(D)$-modules. It follows from Theorem 2.10 that all of the minimal left ideals of A are isomorphic as A-modules. If $A \cong M_n(D)$, then $D^{\mathrm{opp}} \cong \mathrm{End}_{M_n(D)}(D^n) \cong \mathrm{End}_A(I)$, where I is any minimal left ideal of A. The integer n is determined by $[A : k]$. □

[1] The same argument as for finitely generated modules over a field applies over a division algebra.

3 The Brauer group

3.1 Tensor products

Let A and B be k-algebras and let $A \otimes_k B$ be the tensor product of A and B as k-vector spaces. There is a unique k-bilinear multiplication on $A \otimes_k B$ such that $(a \otimes b)(a' \otimes b') = (aa' \otimes bb')$ for all $a, a' \in A$ and $b, b' \in B$. This makes $A \otimes_k B$ into a k-algebra.

Proposition 3.1 (Properties of the tensor product)**.** *Let A and B be central simple k-algebras. Then the following are true:*

(a) $A \otimes_k B \cong B \otimes_k A$.

(b) $(A \otimes_k B) \otimes_k C \cong A \otimes_k (B \otimes_k C)$.

(c) $A \otimes_k M_n(k) \cong M_n(A)$.

(d) For k-algebras A and A' with subalgebras B and B', we have

$$C_{A \otimes_k A'}(B \otimes_k B') = C_A(B) \otimes_k C_{A'}(B').$$

(e) $A \otimes_k B$ is central simple.

(f) $A \otimes_k A^{\mathrm{opp}} \cong \mathrm{End}_k(A) \cong M_n(k)$, *where* $n := \dim_k A$.

Proof. See [1]. All of these are immediate except for (d) and (e). Showing that the product of simple k-algebras is simple requires the notion of primordial elements. In (f), the natural isomorphism $A \otimes_k A^{\mathrm{opp}} \xrightarrow{\sim} \mathrm{End}_k(A)$ is given by $a \otimes a' \mapsto (b \mapsto aba')$. □

3.2 Definition of the Brauer group

Let A and B be central simple k-algebras. We say A and B are *similar* and write $A \sim B$ if $A \otimes_k M_n(k) \cong B \otimes_k M_m(k)$ for some m and n. We denote the equivalence class of a central simple k-algebra A by $[A]$. Let $\mathrm{Br}(k)$ be the set of similarity classes of central simple k-algebras. By Proposition 3.1, the binary operation on $\mathrm{Br}(k)$ defined by $[A] \cdot [B] := [A \otimes_k B]$ is well-defined and makes $\mathrm{Br}(k)$ into an abelian group with identity element $[k]$. The inverse of an element $[A] \in \mathrm{Br}(k)$, is given by $[A^{\mathrm{opp}}]$.

Definition 3.2. *The* Brauer group *of k is the abelian group* $\big(\mathrm{Br}(k), \cdot\big)$.

Remark. In light of the Artin-Wedderburn theorem, we may equivalently define $\mathrm{Br}(k)$ as the set of isomorphism classes of central division algebras over k. Given central division algebras D_1 and D_2, the tensor product $D_1 \otimes D_2$ is isomorphic to $M_n(D_3)$ for some n and central division algebra D_3. The group law is then given by $[D_1] \cdot [D_2] = [D_3]$.

3.3 Extending the base field

Let L/k be a field extension, and let A be central simple over k.

Proposition 3.3. *The tensor product $A \otimes_k L$ is central simple over L.*

Proof. See [1, Lemma 2.15]. □

Definition 3.4. *We say a central simple k-algebra A (or its class in $\mathrm{Br}(k)$) is* split *by L if $A \otimes_k L \cong M_n(L)$ for some n.*

Since $M_n(k) \otimes_k L \cong M_n(L)$ and $(A \otimes_k L) \otimes_L (B \otimes_k L) \cong (A \otimes_k B) \otimes_k L$. We obtain a homomorphism

$$\mathrm{Br}(k) \to \mathrm{Br}(L), \quad [A] \mapsto [A \otimes_k L].$$

We denote its kernel by $\mathrm{Br}(L/k)$. It consists of the elements of $\mathrm{Br}(k)$ which are split by L.

Lemma 3.5. *Let $B \subset A$ be a simple k-subalgebra. Let $C := C_A(B)$. Then*

$$[B : k][C : k] = [A : k].$$

Proof. See [1, Theorem 3.1]. □

Proposition 3.6. *Suppose L is a subfield of A containing k. The following are equivalent.*

(a) $L = C_A(L)$;

(b) $[A : k] = [L : k]^2$;

(c) L *is a maximal commutative subalgebra of* A.

Proof. (a)⇔(b). Clearly $L \subset C(L)$. Then use $[A : k] = [L : k][C(L) : k]$.

(b)⇒(c). Let $L \subset L' \subset A$ be maximal commutative. Then $L' \subset C(L)$; hence

$$[A : k] \geqslant [L : k][L' : k] \geqslant [L : k]^2.$$

Thus $[L' : k] = [L : k]$.

(c)⇒(a). If $L \subsetneq C(L)$, then $L[\gamma]$ is a commutative subalgebra of A for $\gamma \in C(L) \setminus L$. □

Proposition 3.7. *The field L splits A if and only if there exists a $B \sim A$ containing L such that*

$$[B : k] = [L : k]^2.$$

In particular, if $L \subset A$ has degree $[A : k]^{1/2}$ over k, then L splits A.

Proof sketch. If L splits A, then L also splits A^{opp}, so $A^{\text{opp}} \otimes_k L = \text{End}_L(V)$, for some finite dimensional L-vector space V. Define $B := C_{\text{End}_k(V)}(A^{\text{opp}})$. Since $L = C_{\text{End}_k(V)}(A^{\text{opp}} \otimes_k L)$, it follows that $L \subset B$. One can show that B satisfies the required conditions.

For the converse, if suffices to show that L splits B. We have $C_B(L) = L$; hence $C_{B \otimes_k B^{\text{opp}}}(1 \otimes_k L) = B \otimes_k L$. Identifying $B \otimes B^{\text{opp}}$ with $\text{End}_k(B)$ sends $C(1 \otimes L)$ to $\text{End}_L(B)$. Hence $B \otimes_k L \cong \text{End}_L(B)$. □

Corollary 3.8. *Let D be a central division algebra over k such that $[D : k] = [L : k]^2$. The following are equivalent:*

(a) L splits D.

(b) There exists a homomorphism of k-algebras $L \to D$ whose image is a maximal subfield of D.

Proposition 3.9. *Every central division algebra over k contains a maximal* ***separable*** *subfield which is finite over k.*

Proof. See [2, Tag 0752]. □

Theorem 3.10. *We have $\text{Br}(k) = \bigcup_L \text{Br}(L/k)$, where L runs over all finite Galois extensions in k^{sep}.*

Proof. By Corollary 3.8 and Proposition 3.9, every central division algebra D is split by a finite separable extension of k; hence by a Galois extension. □

4 $\text{Br}(k)$ and Galois cohomology

Let L/k be a finite Galois field extension, and let $G := \text{Gal}(L/k)$. Let $\mathcal{A}(L/k)$ denote the set of central simple k-algebras A containing L such that $C_A(L) = L$.

Theorem 4.1 (Noether-Skolem)**.** *Let $f, g \colon A \to B$ be homomorphisms of k-algebras. If A is simple and B is central simple, then there exists an invertible element $b \in B$ such that $f(a) = b \cdot g(a) \cdot b^{-1}$ for all $a \in A$.*

Proof sketch. If $B = M_n(k)$, then f and g define actions of A on k^n. Let V_f and V_g denote k^n with these actions. Any two A-modules with the same dimension are isomorphic. (This follows from the fact that all A-modules are semisimple and all simple A-modules are isomorphic. See [1, Corollary 1.9].) Thus $\exists b \in B$ such that $f(a) \cdot b = b \cdot g(a)$ for all $a \in A$.

In general, use the fact that $B \otimes B^{\text{opp}}$ is a matrix algebra over k and consider $f \otimes 1, g \otimes 1 \colon A \otimes B^{\text{opp}} \to B \otimes B^{\text{opp}}$. Then $\exists b \in B \otimes B^{\text{opp}}$ which conjugates $f \otimes 1$ to $g \otimes 1$. Show that $b \in C_{B \otimes B^{\text{opp}}}(k \otimes B^{\text{opp}}) = B \otimes k$. Then $b = b_0 \otimes 1$ and b_0 does the job. □

Corollary 4.2. *Let B be a central simple k-algebra, and let A_1 and A_2 be simple k-subalgebras of A. Any isomorphism $f\colon A_1 \to A_2$ is induced by an inner automorphism of A.*

Construction 1. Fix $A \in \mathcal{A}(L/k)$. For every $\sigma \in G$, there exists by Corollary 4.2 an element $e_\sigma \in A^\times$ such that

$$\sigma a = e_\sigma a e_\sigma^{-1}, \quad \text{for all } a \in L \subset A. \tag{4.1}$$

If $f_\sigma \in A$ also satisfies (4.1), then for all $a \in L$ we have

$$f_\sigma^{-1} e_\sigma a = a f_\sigma^{-1} e_\sigma.$$

It follows that $f_\sigma^{-1} e_\sigma \in C_A(L) = L$; and hence $f_\sigma^{-1} e_\sigma \in L^\times$. Fix a choice of e_σ for each $\sigma \in G$. Since $e_\sigma e_\tau$ satisfies (4.1) for $\sigma\tau$, it follows that

$$e_\sigma e_\tau = \varphi(\sigma, \tau) e_{\sigma\tau} \tag{4.2}$$

for some $\varphi(\sigma, \tau) \in L^\times$. We thus obtain a map

$$\varphi\colon G \times G \to L^\times, \quad (\sigma, \tau) \mapsto \varphi(\sigma, \tau).$$

Proposition 4.3. *The map φ is a 2-cocycle.*

Proof. We must verify that $d\varphi = 1$, which in this case amounts to showing that

$$\rho\varphi(\sigma, \tau) \cdot \varphi(\rho, \sigma\tau) = \varphi(\rho, \sigma)\varphi(\rho\sigma, \tau). \tag{4.3}$$

This follows from the associative law:

$$e_\rho(e_\sigma e_\tau) = e_\rho(\varphi(\sigma, \tau) e_{\sigma\tau}) = \rho\varphi(\sigma, \tau) \cdot \varphi(\rho, \sigma\tau) \cdot e_{\rho\sigma\tau}.$$

and

$$(e_\rho e_\sigma) e_\tau = \varphi(\rho, \sigma) e_{\rho\sigma} e_\tau = \varphi(\rho, \sigma)\varphi(\rho\sigma, \tau) \cdot e_{\rho\sigma\tau}.$$

□

A different choice of e_σ's leads to a cohomologous cocycle, and we thereby obtain a well-defined map

$$\tilde{\gamma}\colon \mathcal{A}(L/k) \to H^2(G, L^\times). \tag{4.4}$$

Lemma 4.4. *The $(e_\sigma)_{\sigma \in G}$ form an L-basis for A.*

Proof. See [1, Lemma 3.12]. For dimension reasons, it suffices to show that the e_σ are linearly independent. □

Proposition 4.5. *Let $A, A' \in \mathcal{A}(L/k)$. Then $A \cong A'$ if and only if $\tilde{\gamma}(A) = \tilde{\gamma}(A')$.*

Proof. By Lemma 4.4, the algebra A is uniquely determined by $(e_\sigma)_\sigma$ and the multiplication given by (4.1) and (4.2). If $\tilde{\gamma}(A) = \tilde{\gamma}(A')$, then the map

$$A \to A', \quad \sum_\sigma \ell_\sigma e_\sigma \mapsto \sum_\sigma \ell_\sigma e'_\sigma$$

is an isomorphism of k-algebras. Conversely, suppose there is an isomorphism $f\colon A \xrightarrow{\sim} A'$. Using the Noether-Skolem theorem, after conjugating by an element of A' we may assume that $f(L) = L$ and $f|_L = \mathrm{id}_L$. Then $(f(e_\sigma))_\sigma$ satisfies (4.1) and (4.2) and defines the same cocycle. □

We thus obtain an injective map

$$\gamma\colon \mathcal{A}(L/k)/_{\cong} \hookrightarrow H^2(G, L^\times). \tag{4.5}$$

Our aim is to show that γ is bijective. To do this, we construct an inverse.

Definition 4.6. *A 2-cocycle $\varphi\colon G \times G \to L^\times$ is* normalized *if $\varphi(1,1) = 1$.*

Every cohomology class contains a normalized 2-cycle. Indeed, given a 2-cocycle φ, we can twist by dg, for $g\colon G \to L^\times$, $\sigma \mapsto \varphi(1,1)$, to obtain a normalized one.

Construction 2. Let $\varphi\colon G\times G \to L^\times$ be a normalized cocycle. Let $A(\varphi) := \bigoplus_{\sigma\in G} Le_\sigma$. We make $A(\varphi)$ into a k-algebra by endowing it with the multiplication induced by (4.1) and (4.2). Since φ is normalized, equation (4.2) implies that $\varphi(1,\sigma) = \varphi(\sigma, 1) = 1$ for all $\sigma \in G$; hence e_1 acts as the multiplicative identity. The cocycle condition (4.3) says that $A(\varphi)$ is associative. We identify L with the subfield Le_1 of $A(\varphi)$.

Proposition 4.7. *The algebra $A(\varphi)$ is in $\mathcal{A}(L/k)$.*

Proof. Let $a = \sum_\sigma \ell_\sigma e_\sigma \in A(\varphi)$ and let $\ell \in L$. Comparing $\ell a = \sum_\sigma \ell\ell_\sigma e_\sigma$ and $a\ell = \sum_\sigma \ell_\sigma \sigma\ell e_\sigma$, we see that $a \in C_{A(\varphi)}(L)$ if and only if $a = \ell_1 e_1 \in L$. Hence $C_{A(\varphi)}(L) = L$. Similarly, if $a \in Z(A(\varphi)) \subset L$, then for all $\sigma \in G$, we have $ae_\sigma = e_\sigma a = (\sigma a)e_\sigma$. Thus $a \in k$, and $A(\varphi)$ is central. For the simplicity, see [1, Lemma 3.13]. □

Proposition 4.8. *Let φ and φ' be cohomologous 2-cocycles. Then the k-algebras $A(\varphi) \cong A(\varphi')$ are isomorphic.*

Proof sketch. If φ and φ' are cohomologous, then there exists $a\colon G \to L^\times$ such that

$$a(\sigma)\cdot \sigma a(\tau) \cdot \varphi'(\sigma,\tau) = a(\sigma\tau)\cdot \varphi(\sigma,\tau).$$

The map $A(\varphi) \to A(\varphi')$, $e_\sigma \mapsto a(\sigma)e'_\sigma$ is a k-algebra isomorphism. □

We thus obtain a map

$$\alpha\colon H^2(G, L^\times) \to \mathcal{A}(L/k)/_{\cong}, \quad [\varphi] \mapsto A(\varphi). \tag{4.6}$$

which is inverse to (4.5). By Propositions 3.6 and 3.7, if $A \in \mathcal{A}(L/k)$, then L splits A. We thus have a natural map

$$\mathcal{A}(L/k)/_{\cong} \mapsto \mathrm{Br}(L/k), \quad A \mapsto [A]. \tag{4.7}$$

Theorem 4.9. *The map* $H^2(G, L^\times) \to \mathrm{Br}(L/k)$, $[\varphi] \mapsto [A(\varphi)]$ *is a bijection.*

Proof sketch. It suffices to show that (4.7) is bijective.

Injectivity. If $A \sim A'$, there is a central division algebra D such that $A \sim D \sim A'$, i.e. $A \cong M_n(D)$ and $A' \cong M_n'(D)$. Since $[A : k] = [L : k]^2 = [A' : k]$, it follows that $n = n'$, so $A \cong A'$.

Surjectivity. Follows directly from Proposition 3.7. □

Let $G_k := \mathrm{Gal}(k^{\mathrm{sep}}/k)$.

Corollary 4.10. *There is a natural bijection* $H^2(G_k, (k^{\mathrm{sep}})^\times) \xrightarrow{\sim} \mathrm{Br}(k)$.

Proof sketch. For every tower of $E \supset L \supset k$ of Galois extensions of k, the diagram

$$\begin{array}{ccc} H^2(L/k) & \longrightarrow & \mathrm{Br}(L/k) \\ \downarrow & & \downarrow \\ H^2(E/k) & \longrightarrow & \mathrm{Br}(E/k). \end{array}$$

commutes. Take inductive limits (use Theorem 3.10). □

References

[1] Milne, J.S.: *Class Field Theory.* https://www.jmilne.org/math/CourseNotes/CFT.pdf (March 2013).

[2] Stacks Project Authors: *Stacks Project.* https://stacks.math.columbia.edu (2018).