NOTES ON NONCOMMUTATIVE ALGEBRA

TAMÁS SZAMUELY

Most of the material in these notes comes from my book with Philippe Gille, *Central Simple Algebras and Galois Cohomology*, 2nd ed., Cambridge University Press, 2017. However, sometimes I take a different approach from that of the book.

CONTENTS

1. THE WEDDERBURN–ARTIN THEOREM

Let R be a not necessarily commutative ring with unit. The ring R is *simple* if it has no two-sided ideal other than 0 and R.

Example 1.1. Assume D is a ring such that every element $x \in D$ has a two-sided inverse (i.e. $y \in D$ such that $xy = yx = 1$). In this case D is called a *division algebra* or a *skew field*; it is obviously a simple ring. Note that the centre $Z(D)$ of elements commuting with all elements of D is a nontrivial subring and also a field (indeed, inverting the relation $xy = yx$ gives $y^{-1}x^{-1} = x^{-1}y^{-1}$ for all $y \in D, x \in Z(D)$). Hence D is indeed an algebra over $Z(D)$.

We now give concrete examples of division algebras.

Example 1.2. Let k be a field. For any two elements $a, b \in k^\times$ define the *(generalized) quaternion algebra* (a, b) as the 4-dimensional k-algebra with basis $1, i, j, ij$, multiplication being determined by

$$i^2 = a, \;\; j^2 = b, \;\; ij = -ji.$$

One calls the set $\{1, i, j, ij\}$ a *quaternion basis* of (a, b).

Given an element $q = x + yi + zj + wij$ of the quaternion algebra (a, b), we define its *conjugate* by

$$\overline{q} = x - yi - zj - wij.$$

The map $(a, b) \to (a, b)$ given by $q \mapsto \overline{q}$ is an anti-automorphism of the k-algebra (a, b), i.e. it is a k-vector space automorphism of (a, b) satisfying $\overline{(q_1 q_2)} = \overline{q}_2 \overline{q}_1$. Moreover, we have $\overline{\overline{q}} = q$; an anti-automorphism with this property is called an *involution* in ring theory.

We define the *norm* of $q = x + yi + zj + wij$ by $N(q) = q\overline{q}$. A calculation yields

$$N(q) = x^2 - ay^2 - bz^2 + abw^2 \in k, \tag{1}$$

so $N : (a, b) \to k$ is a *nondegenerate quadratic form*. The computation

$$N(q_1 q_2) = q_1 q_2 \overline{q}_2 \overline{q}_1 = q_1 N(q_2) \overline{q}_1 = N(q_1) N(q_2)$$

shows that the norm is a multiplicative function. If $N(q) \neq 0$, then $\overline{q} N(q)^{-1}$ is a two-sided inverse for q. Thus an element q of the quaternion algebra (a, b) is invertible if and only if it has nonzero norm. Hence (a, b) is a division algebra if and only if the norm $N : (a, b) \to k$ does not vanish outside 0.

The classical example is that of *Hamilton quaternions* where $k = \mathbf{R}$ and $a = b = -1$. In this case $N(q) = x^2 + y^2 + z^2 + w^2$ for all q, so we indeed have a division algebra over $\mathbf{R}$.

The next example allows us to construct more examples of simple rings.

Example 1.3. If D is a division algebra over k, the ring $M_n(D)$ of $n \times n$ matrices over D is simple for all $n \geq 1$. Checking this is an exercise in matrix theory. Indeed, we have to show that the two-sided ideal $\langle M \rangle$ in $M_n(D)$ generated by a nonzero matrix M is $M_n(D)$ itself. Consider the matrices E_{ij} having 1 as the j-th element of the i-th row and zero elsewhere. Since each element of $M_n(D)$ is a D-linear combination of the E_{ij}, it suffices to show that $E_{ij} \in \langle M \rangle$ for all i, j. But in view of the relation $E_{ki} E_{ij} E_{jl} = E_{kl}$ we see that it is enough to show $E_{ij} \in \langle M \rangle$ for *some* i, j. Now choose i, j so that the j-th element in the i-th row of M is a nonzero element m. Then $m^{-1} E_{ii} M E_{jj} = E_{ij}$, and we are done.

Notice also that, since in a matrix ring the centre can only contain scalar multiples of the identity matrix, the centre of $M_n(D)$ equals that of D.

The main theorem of this section provides a converse to the above example. Call a ring *Artinian* if its left ideals satisfy the descending chain condition.

Theorem 1.4. (Wedderburn–Artin) *Let R be a simple Artinian ring. Then there exist an integer $n \geq 1$ and a division algebra D so that R is isomorphic to the matrix ring $M_n(D)$. Moreover, the division algebra D is uniquely determined up to isomorphism.*

Before embarking on the proof we need a couple of lemmas. First recall some basic facts from module theory. First, a nonzero R-module M is *simple* if it has no R-submodules other than 0 and M.

Example 1.5. Let us describe the simple left modules over $M_n(D)$, where D is a division algebra. For all $1 \leq r \leq n$, consider the left ideal $I_r \subset M_n(D)$ formed by matrices $M = [m_{ij}]$ with $m_{ij} = 0$ for $j \neq r$. A simple argument with the matrices E_{ij} of Example 1.3 shows that the I_r are *minimal* left ideals with respect to inclusion, i.e. simple $M_n(D)$-modules. Moreover, we have $M_n(D) = \bigoplus I_r$ and the I_r are all isomorphic as $M_n(D)$-modules. Finally, if M is a simple $M_n(D)$-module, it must be a quotient of $M_n(D)$, but then the induced map $\bigoplus I_r \to M$ must induce an isomorphism with some I_r. Thus all simple left $M_n(D)$-modules are isomorphic to (say) I_1.

An R-module M is *semisimple* if it can be written as a direct sum of simple submodules. By the above example $M_n(D)$ as a module over itself is semisimple; moreover, in this case the simple components are all isomorphic and the direct sum is finite.

Lemma 1.6. *If M is semisimple, then so is every submodule and quotient of M. More precisely, if $M \cong \oplus_{i\in I} M_i$ with M_i simple, then every submodule and quotient is isomorphic to a direct sum of some of the M_i.*

Proof. If $N \subset M$ is a submodule, we find a subset $J \subset I$ such that $N' := \oplus_{i\in J} M_i$ satisfies $N \cap N' = 0$ and J is maximal with this property (for I finite the existence of J is obvious, otherwise we use Zorn's lemma). Then $M = N \oplus N'$. Indeed, if $j \notin J$, then $(N' \oplus M_j) \cap N \neq 0$ by maximality of J and thus there is $n \in N$, $n' \in N'$ and a nonzero $m_j \in M_j$ with $n = n' + m_j$. But then $m_j \in (N + N') \cap M_j$, so since M_j is simple, $M_j \subset N + N'$. As this holds for all j, we get $M = N + N'$ and the sum is direct by construction. Now consider the quotient map $M \twoheadrightarrow M/N'$. For $N'' := \oplus_{i\in I\setminus J} M_i$ we have $N'' \cap N' = 0$ by definition, so N'' maps isomorphically onto $M/N' \cong N$. This shows that $N \cong \oplus_{i\in I\setminus J} M_i$ and $M/N \cong N' \cong \oplus_{i\in J} M_i$, as required. □

Next, an *endomorphism* of a left R-module M over a ring R is an R-homomorphism $M \to M$; these form a ring $\mathrm{End}_R(M)$ where addition is given by the rule $(\phi+\psi)(x) = \phi(x) + \psi(x)$ and multiplication by composition of maps. In the case when R is a division algebra, M is a left vector space over R, so in case it is of finite dimension n, the usual argument from linear algebra shows that choosing a basis of M induces an isomorphism $\mathrm{End}_R(M) \cong M_n(R)$.

Finally, notice that when $R = M$ and $\phi \in \mathrm{End}_R(R)$, then for every $r \in R$ we have $\phi(r) = \phi(r \cdot 1) = r\phi(1)$, so ϕ is given by right multiplication with $\phi(1)$. This shows that there is an isomorphism $\mathrm{End}_R(R) \cong R^\circ$, where R° is the *opposite ring of* R, i.e. the ring which has the same additive structure as R but in which multiplication is given by $(x, y) \mapsto yx$.

Lemma 1.7. (Schur) *Let M be a simple module over a ring R. Then $\mathrm{End}_R(M)$ is a division algebra.*

Proof. The kernel of a nonzero endomorphism $M \to M$ is an R-submodule different from M, hence it is 0. Similarly, its image must be the whole of M. Thus it is an isomorphism, which means it has an inverse in $\mathrm{End}_R(M)$. □

Schur's lemma has the following complement.

Lemma 1.8. *For an arbitrary R-module M and an integer $n > 0$ there is an isomorphism $\mathrm{End}_R(M^n) \cong M_n(D)$, where $D = \mathrm{End}_R(M)$.*

Proof. To distinguish components of M^n, write $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$ with $M_i = M$ for all i. If $\phi \in \mathrm{End}_R(M^n)$ and $1 \leq i, j \leq n$, consider the composite map $M_i \to \oplus_i M_i \xrightarrow{\phi} \oplus_i M_i \to M_j$ where the first map is the natural inclusion and the last one is the projection. We obtain a map $\phi_{ij} : M_i \to M_j$ which may be identified with an element of $D = \mathrm{End}_R(M)$. The $n \times n$ matrix of the ϕ_{ij} defines an element of $M_n(D)$; conversely, such a matrix defines an element in $\mathrm{End}_R(M^n)$. The reader will check that this bijection is compatible with the ring operations on both sides. □

Proof of Theorem 1.4: As R is Artinian, a descending chain of left ideals must stabilize. So let L be a minimal left ideal; it is then a simple R-module. We first show that $R \cong L^n$ for some $n > 0$. Consider all possible R-module homomorphisms $R \to L^m$ for some $m > 0$ and let ρ be one such homomorphism with minimal kernel (such a ρ exists as R is Artinian). We show $\ker(\rho) = 0$, which will imply the claim because then R identifies with a submodule of the semisimple module L^m and we may apply Lemma 1.6. Suppose $\ker(\rho) \neq 0$ and pick a nonzero $r_0 \in \ker(\rho)$. Now look at $\mathrm{Ann}(L) := \{r \in R : rL = 0\}$. This is a two-sided ideal in R that does not contain 1, so it is 0 because R is simple. In particular, for r_0 we find $l_0 \in L$ such that $r_0 l_0 \neq 0$. But then $\tilde{\rho} : R \to L^m \oplus L$ given by $r \mapsto (\rho(r), rl_0)$ has smaller kernel, a contradiction.

By Schur's lemma, $D = \mathrm{End}_R(L)$ is a division algebra, and by Lemma 1.8 we have $\mathrm{End}_R(R) \cong \mathrm{End}_R(L^n) \cong M_n(D)$. But we know $\mathrm{End}_R(R) \cong R^\circ$, so finally $R \cong M_n(D^\circ)$.

For the uniqueness statement, assume that D and D' are division algebras for which $R \cong M_n(D) \cong M_m(D')$ with suitable integers n, m. By Example 1.5, the minimal left ideal L then satisfies $D^n \cong L \cong D'^m$, whence a chain of isomorphisms $D \cong \mathrm{End}_R(D^n) \cong \mathrm{End}_R(L) \cong \mathrm{End}_R(D'^m) \cong D'$. □

Remark 1.9. More generally, a ring R is called semisimple if it is semisimple as an R-module, i.e. it can be written as a direct sum of minimal left ideals (possibly with multiplicity). If moreover R is Artinian, the direct sum must be finite and then the above proof shows that R is isomorphic to a finite direct product of matrix algebras over division algebras.

Now suppose k is a field. A *central simple k-algebra* is a finite dimensional simple k-algebra whose centre is k. By finite dimensionality such a k-algebra is necessarily an Artinian ring. Theorem 1.4 for central simple algebras is the case originally proven by Wedderburn, so we'll frequently refer to the statement as Wedderburn's theorem.

Corollary 1.10. *If k is algebraically closed, every central simple k-algebra is isomorphic to $M_n(k)$ for some $n \geq 1$.*

Proof. By the theorem it is enough to see that there is no finite dimensional division algebra $D \supset k$ other than k. For this, let d be an element of $D \setminus k$. As D is finite dimensional over k, the powers $\{1, d, d^2, \dots\}$ are linearly dependent, so there is a polynomial $f \in k[x]$ with $f(d) = 0$. As D is a division algebra, it has no zero divisors and we may assume f irreducible. This means there is a k-algebra homomorphism $k[x]/(f) \to D$ which realises the field $k(d)$ as a k-subalgebra of D. But k being algebraically closed, we have $k[x]/(f) \cong k$, so $k(d) = k$. □

2. Splitting fields and the Brauer group

The last corollary enables one to give an alternative characterization of central simple algebras.

Theorem 2.1. *Let k be a field and A a finite dimensional k-algebra. Then A is a central simple algebra if and only if there exist an integer $n > 0$ and a finite field extension $K|k$ so that $A \otimes_k K$ is isomorphic to the matrix ring $M_n(K)$.*

We first prove:

Lemma 2.2. *Let A be a finite dimensional k-algebra, and $K|k$ an algebraic field extension. The algebra A is central simple over k if and only if $A \otimes_k K$ is central simple over K.*

Proof. If I is a nontrivial (two-sided) ideal of A, then $I \otimes_k K$ is a nontrivial ideal of $A \otimes_k K$ (e.g. for dimension reasons); similarly, if A is not central, then neither is $A \otimes_k K$. Thus if $A \otimes_k K$ is central simple, then so is A.

To prove the converse, we first reduce to the case of a finite extension $K|k$. For this, we write $K|k$ as a union of its finite subextensions $K'|K$ and observe that every ideal $I \subset A \otimes_k K$ is the union of the ideals $I \cap K' \subset A \otimes_k K'$; moreover, we have $Z(A \otimes_k K) \subset Z(A \otimes_k K')$ for any K'. Next, using Wedderburn's theorem we may assume that $A = D$ is a division algebra. Under this assumption, if $w_1, \dots, w_n$ is a k-basis of K, then $1 \otimes w_1, \dots, 1 \otimes w_n$ yields a D-basis of $D \otimes_k K$ as a left D-vector space. Given an element $x = \sum \alpha_i (1 \otimes w_i)$ in the centre of $D \otimes_k K$, for all $d \in D$ the relation $x = (d^{-1} \otimes 1)x(d \otimes 1) = \sum (d^{-1}\alpha_i d)(1 \otimes w_i)$ implies $d^{-1}\alpha_i d = \alpha_i$ by the linear independence of the $1 \otimes w_i$. As D is central over k, the α_i must lie in k, so $D \otimes_k K$ is central over K. Now if J is a nonzero ideal in $D \otimes_k K$ generated by elements $z_1, \dots, z_r$, we may assume the z_i to be D-linearly independent and extend them to a D-basis of $D \otimes_k K$ by adjoining some of the $1 \otimes w_i$, say $1 \otimes w_{r+1}, \dots, 1 \otimes w_n$. Thus for $1 \leq i \leq r$ we may write

$$1 \otimes w_i = \sum_{j=r+1}^{n} \alpha_{ij}(1 \otimes w_j) + y_i,$$

where y_i is some D-linear combination of the z_i and hence an element of J. Here $y_1, \dots, y_r$ are D-linearly independent (because so are $1 \otimes w_1, \dots, 1 \otimes w_r$), so they form a D-basis of J. As J is a two-sided ideal, for all $d \in D$ we must have $d^{-1}y_i d \in J$ for $1 \leq i \leq r$, so there exist $\beta_{il} \in D$ with $d^{-1}y_i d = \sum \beta_{il} y_l$. We may rewrite this relation as

$$(1 \otimes w_i) - \sum_{j=r+1}^{n} (d^{-1}\alpha_{ij}d)(1 \otimes w_j) = \sum_{l=1}^{r} \beta_{il}(1 \otimes w_l) - \sum_{l=1}^{r} \beta_{il} \sum_{j=r+1}^{n} \alpha_{lj}(1 \otimes w_j),$$

from which we get as above, using the independence of the $1 \otimes w_j$, that $\beta_{ii} = 1$, $\beta_{il} = 0$ for $l \neq i$ and $d^{-1}\alpha_{ij}d = \alpha_{ij}$, i.e. $\alpha_{ij} \in k$ as D is central. This means that J can be generated by elements of K (viewed as a k-subalgebra of $D \otimes_k K$ via the embedding $w \mapsto 1 \otimes w$). As K is a field, we must have $J \cap K = K$, so $J = D \otimes_k K$. This shows that $D \otimes_k K$ is simple. □

Proof of Theorem 2.1: Sufficiency follows from the above lemma and Example 1.3. For necessity, note first that denoting by $\overline{k}$ an algebraic closure of k, the lemma together with Corollary 1.10 imply that $A \otimes_k \overline{k} \cong M_n(\overline{k})$ for some n. Now observe that for every finite field extension K of k contained in $\overline{k}$, the inclusion $K \subset \overline{k}$ induces an injective map $A \otimes_k K \to A \otimes_k \overline{k}$ and $A \otimes_k \overline{k}$ arises as the union of the $A \otimes_k K$ in this way. Hence for a sufficiently large finite extension $K|k$ contained

in $\overline{k}$ the algebra $A \otimes_k K$ contains the elements $e_1, \ldots, e_{n^2} \in A \otimes_k \overline{k}$ corresponding to the standard basis elements of $M_n(\overline{k})$ via the isomorphism $A \otimes_k \overline{k} \cong M_n(\overline{k})$, and moreover the elements a_{ij} occurring in the relations $e_i e_j = \sum a_{ijl} e_l$ defining the product operation are also contained in K. Mapping the e_i to the standard basis elements of $M_n(K)$ then induces a K-isomorphism $A \otimes_k K \cong M_n(K)$. □

Corollary 2.3. *If A is a central simple k-algebra, its dimension over k is a square.*

Definition 2.4. A field extension $K|k$ over which $A \otimes_k K$ is isomorphic to $M_n(K)$ for suitable n is called a *splitting field* for A. We shall also employ the terminology *A splits over K* or *K splits A*.

The integer $\sqrt{\dim_k A}$ is called the *degree* of A.

Example 2.5. Every quaternion algebra over a field k is a central simple algebra of degree 2. To see this, we first show that the matrix algebra $M_2(k)$ is isomorphic to a quaternion algebra over k. Indeed, for every $b \in k^\times$ the assignment

$$i \mapsto I := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad j \mapsto J := \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}$$

defines an isomorphism $(1, b) \cong M_2(k)$, because the matrices

$$\text{(2)} \qquad \mathrm{Id} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; I = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \; J = \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix} \text{ and } IJ = \begin{bmatrix} 0 & b \\ -1 & 0 \end{bmatrix}$$

generate $M_2(k)$ as a k-vector space, and they satisfy the relations

$$I^2 = \mathrm{Id}, \quad J^2 = b\,\mathrm{Id}, \quad IJ = -JI.$$

Next, notice that for any $a, b, u \in k^\times$ we have an isomorphism $(a, b) \cong (u^2 a, u^2 b)$ induced by the substitutions $i \mapsto ui$, $j \mapsto uj$. So if $a \in k^{\times 2}$, then $(a, b) \cong (1, a^{-1}b) \cong M_2(k)$. But if $a \notin k^{\times 2}$, we at least have $a \in k(\sqrt{a})^{\times 2}$, so $(a, b) \otimes_k k(\sqrt{a}) \cong M_2(k(\sqrt{a}))$ and (a, b) is a central simple algebra by Theorem 2.1.

Moreover, Wedderburn's theorem implies that (a, b) is either split or a division algebra.

Given Theorem 2.1, we can easily prove:

Lemma 2.6. *If A and B are central simple k-algebras split by K, then so is $A \otimes_k B$.*

Proof. In view of the isomorphism $(A \otimes_k K) \otimes_K (B \otimes_k K) \cong (A \otimes_k B) \otimes_k K$ and Theorem 2.1, it is enough to verify the isomorphism of matrix algebras $M_n(K) \otimes_K M_m(K) \cong M_{nm}(K)$. Perhaps the simplest argument for this is to note that given K-endomorphisms $\phi \in \mathrm{End}_K(K^n)$ and $\psi \in \mathrm{End}_K(K^m)$, the pair (ϕ, ψ) induces an

element $\phi \otimes \psi$ of $\mathrm{End}_K(K^n \otimes_K K^m)$. The resulting map $\mathrm{End}_K(K^n) \otimes \mathrm{End}_K(K^m) \to \mathrm{End}_K(K^n \otimes_K K^m)$ is obviously injective, and it is surjective e.g. by dimension reasons. □

Recall that the *opposite algebra* A° of a k-algebra A is the k-algebra with the same underlying k-vector space as A, but in which the product of two elements x, y is given by the element yx with respect to the product in A. If A is central simple over k, then so is A°. By the lemma, their tensor product is again central simple, but more is true:

Proposition 2.7. *There is a canonical isomorphism $A \otimes_k A^\circ \xrightarrow{\sim} \mathrm{End}_k(A)$ of k-algebras. Consequently, $A \otimes_k A^\circ$ is isomorphic to the matrix algebra $M_{n^2}(k)$, where n is the degree of A.*

Proof. Define a k-linear map $A \otimes_k A^\circ \to \mathrm{End}_k(A)$ by sending $\sum a_i \otimes b_i$ to the k-linear map $x \mapsto \sum a_i x b_i$. This map is manifestly nonzero, and hence injective, because $A \otimes_k A^\circ$ is simple by Lemma 2.6. Thus it is an isomorphism for dimension reasons. □

Consider now the following construction.

Construction 2.8. Two central simple k-algebras A and A' are called *Brauer equivalent* or *similar* if $A \otimes_k M_m(k) \cong A' \otimes_k M_{m'}(k)$ for some $m, m' > 0$. This defines an equivalence relation on the family of central simple k-algebras split by a fixed finite extension $K|k$. We denote the set of equivalence classes by $\mathrm{Br}(K|k)$ and the union of the sets $\mathrm{Br}(K|k)$ for all finite Galois extensions by $\mathrm{Br}(k)$.

Remarks 2.9. Brauer equivalence enjoys the following basic properties.

(1) One sees from the definition that each Brauer equivalence class contains (up to isomorphism) a unique division algebra. Thus we can also say that $\mathrm{Br}(K|k)$ classifies division algebras split by K.
(2) It follows from Wedderburn's theorem and the previous remark that if A and B are two Brauer equivalent k-algebras of the same dimension, then $A \cong B$.

The set $\mathrm{Br}(K|k)$ (and hence also $\mathrm{Br}(k)$) is equipped with a product operation induced by the tensor product of central simple k-algebras; indeed, the tensor product preserves Brauer equivalence.

Proposition 2.10. *The sets $\mathrm{Br}(K|k)$ and $\mathrm{Br}(k)$ equipped with the above product operation are abelian groups.*

Proof. Basic properties of the tensor product imply that the product operation is commutative and associative. If A represents a class in $\mathrm{Br}(K|k)$, the class of the opposite algebra A° yields an inverse in view of Proposition 2.7. □

Definition 2.11. We call $\mathrm{Br}(K|k)$ equipped with the above product operation the *Brauer group of k relative to K* and $\mathrm{Br}(k)$ the *Brauer group* of k.

To study the Brauer group we need the following crucial theorem.

Theorem 2.12. *Every central division algebra D of degree n over an infinite field k is split by a separable extension $K|k$ of degree n. Moreover, such a K may be found among the k-subalgebras of D.*

Remark 2.13. We shall prove in Example 4.13 below that over a finite field every central simple algebra is split. Without using this result, we can still make a straightforward remark: since a finite field is perfect, every central simple algebra over it is split by a finite separable extension.

Theorem 2.12 is an immediate consequence of Propositions 2.14 and 2.15 below that are interesting in their own right.

Proposition 2.14. *If a central simple k-algebra A of degree n contains a k-subalgebra K which is a degree n field extension of k, then A splits over K.*

Proof. Let A° be the opposite algebra to A. By Proposition 2.7 we have an isomorphism $A \otimes_k A^\circ \cong \mathrm{End}_k(A)$. If K is as above, the inclusion $K \subset A$ induces an inclusion $K \subset A^\circ$ by commutativity of K, whence also an injection $\iota : A \otimes_k K \to \mathrm{End}_k(A)$. Viewing A as a K-vector space with K acting via right multiplication, the construction of the map $A \otimes_k A^\circ \to \mathrm{End}_k(A)$ in the proof of Proposition 2.7 shows that the image of ι lies in $\mathrm{End}_K(A)$. By definition, we have $\mathrm{End}_K(A) \cong M_n(K)$; in particular, it has dimension n^2 over K. On the other hand, we have $\dim_K(A \otimes_k K) = \dim_k(A) = n^2$, so the map $\iota : A \otimes_k K \to \mathrm{End}_K(A)$ is an isomorphism. □

Proposition 2.15. *If D is as in the theorem, then D contains an element $a \in D$ such that the field extension $k(a)|k$ is separable of degree n.*

Proof. By Corollary 1.10 there is an isomorphism $\phi : D \otimes_k \overline{k} \cong M_d(\overline{k})$. Identify $M_d(\overline{k})$ with points of the affine space $\mathbf{A}^{d^2}_{\overline{k}}$ via the standard basis, and consider the subset U of matrices with separable characteristic polynomial. These form a Zariski open set because if we identify the set of degree d monic polynomials in $\overline{k}[x]$ with points of $\mathbf{A}^d_{\overline{k}}$ via $x^d + a_{d-1}x^{d-1} + \cdots + a_0 \mapsto (a_{d-1}, \ldots, a_0)$ the separable polynomials correspond to the Zariski open set given by the nonvanishing of the discriminant; the set U is the preimage of this open set by the morphism $\mathbf{A}^{d^2}_{\overline{k}} \to \mathbf{A}^d_{\overline{k}}$ sending a matrix to

its characteristic polynomial, modulo the above identifications. Now identify the elements of $D \otimes_k \overline{k}$ with the points of $\mathbf{A}^{d^2}_{\overline{k}}$ in such a way that the elements of D correspond to the k-points of the affine space $\mathbf{A}^{d^2}_k$. As k is infinite, the open subset $\phi^{-1}(U) \subset \mathbf{A}^{d^2}_{\overline{k}}$ contains a k-rational point of $\mathbf{A}^{d^2}$ (this fact holds for every nonempty Zariski open subset and is promptly verified by reducing to the case $d = 1$). This point in turn corresponds to an element $a \in D$. By construction, over $\overline{k}$ it yields a matrix $M = \phi(a \otimes 1)$ whose characteristic polynomial P has distinct roots, hence P is also the minimal polynomial of M. This minimal polynomial is the same as that of the $\overline{k}$-linear extension L_M of the left multiplication map $L_a : D \to D, x \mapsto ax$ to $M_d(\overline{k})$ via ϕ, as L_M is given via left multiplication by the block diagonal matrix $\mathrm{diag}(M, \ldots, M)$. But the minimal polynomial does not change by base extension (see e.g. S. Lang, *Algebra*, Chapter XIV, Corollary 2.2), so the k-linear map L_a also has the separable polynomial P as its minimal polynomial; in particular, P has coefficients in k. Finally, the minimal polynomial of the map L_a is the same as the minimal polynomial of $a \in D$ over k, which is irreducible as D is a division algebra. So the homomorphism $k[x] \to D$ sending x to d induces the required embedding $k(d) \hookrightarrow D$. □

Corollary 2.16. (Noether, Köthe) *A central simple k-algebra has a splitting field that is finite and separable over k.*

Proof. Combine Theorem 2.12 (and Remark 2.13) with Wedderburn's theorem. □

Corollary 2.17. *A finite dimensional k-algebra A is a central simple algebra if and only if there exist an integer $n > 0$ and a finite* Galois *field extension $K|k$ so that $A \otimes_k K$ is isomorphic to the matrix ring $M_n(K)$.*

Proof. The 'if' part is contained in Theorem 2.1. The 'only if' part follows from the previous corollary together with the well-known fact from Galois theory according to which every finite separable field extension embeds in a finite Galois extension. □

Remarks 2.18.

(1) It is important to bear in mind that if A is a central simple k-algebra of degree n which does not split over k but splits over a finite Galois extension $K|k$ with group G, then the isomorphism $A \otimes_k K \cong M_n(K)$ is *not* G-equivariant if we equip $M_n(K)$ with the usual action of G coming from its action on K. Indeed, were it so, we would get an isomorphism $A \cong M_n(k)$ by taking G-invariants.

(2) It is not always possible to realize a Galois splitting field as a k-subalgebra in a central simple algebra, as shown by a famous counterexample by Amitsur. Central simple algebras containing a Galois splitting field are called *crossed products* in the literature.

3. GALOIS DESCENT

Corollary 2.17 makes it possible to classify central simple algebras using methods of Galois theory. Here we present such a method, known as *Galois descent*.

We shall work in a more general context, that of *vector spaces V equipped with a tensor Φ of type (p, q)*. By definition, Φ is an element of the tensor product $V^{\otimes p} \otimes_k (V^*)^{\otimes q}$, where $p, q \geq 0$ are integers and V^* is the dual space $\mathrm{Hom}_k(V, k)$. Note the natural isomorphism

$$V^{\otimes p} \otimes_k (V^*)^{\otimes q} \cong \mathrm{Hom}_k(V^{\otimes q}, V^{\otimes p})$$

coming from the general formula $\mathrm{Hom}_k(V, k) \otimes_k W \cong \mathrm{Hom}_k(V, W)$.

Examples 3.1. Some of the most important special cases are:

- The trivial case $\Phi = 0$ (with any p, q). This is just V with no additional structure.
- $p = 1, q = 1$. In this case Φ is given by a k-linear endomorphism of V.
- $p = 0, q = 2$. Then Φ is a sum of tensor products of k-linear functions, i.e. a k-bilinear form $V \otimes_k V \to k$.
- $p = 1, q = 2$. This case corresponds to a k-bilinear map $V \otimes_k V \to V$.

Note that the theory of associative algebras is contained in the last example, for the multiplication in such an algebra A is given by a k-bilinear map $A \otimes_k A \to A$ satisfying the associativity condition.

So consider pairs (V, Φ) of k-vector spaces equipped with a tensor of fixed type (p, q) as above. A k-isomorphism between two such objects (V, Φ) and (W, Ψ) is given by a k-isomorphism $f : V \tilde{\to} W$ of k-vector spaces such that $f^{\otimes q} \otimes (f^{*-1})^{\otimes q} : V^{\otimes p} \otimes_k (V^*)^{\otimes q} \to W^{\otimes p} \otimes_k (W^*)^{\otimes q}$ maps Φ to Ψ. Here $f^* : W^* \tilde{\to} V^*$ is the k-isomorphism induced by f.

Now fix a finite Galois extension $K|k$ with Galois group $G = \mathrm{Gal}(K|k)$. Denote by V_K the K-vector space $V \otimes_k K$ and by Φ_K the tensor induced on V_K by Φ. In this way we associate with (V, Φ) a K-object (V_K, Φ_K). We say that (V, Φ) and (W, Ψ) *become isomorphic over K* if there exists a K-isomorphism between (V_K, Φ_K) and (W_K, Ψ_K). In this situation, (W, Ψ) is also called a *$(K|k)$-twisted form* of (V, Φ) or a *twisted form* for short.

Now Galois theory enables one to classify k-isomorphism classes of twisted forms as follows. Given a k-automorphism $\sigma : K \to K$, tensoring by V gives a k-automorphism $V_K \to V_K$ which we again denote by σ. Each K-linear map $f : V_K \to W_K$ induces a map $\sigma(f) : V_K \to W_K$ defined by $\sigma(f) = \sigma \circ f \circ \sigma^{-1}$. If f is a K-isomorphism from (V_K, Φ_K) to (W_K, Ψ_K), then so is $\sigma(f)$. The map $f \to \sigma(f)$ preserves composition of automorphisms, hence we get a *left action* of $G = \mathrm{Gal}(K|k)$ on the group $\mathrm{Aut}_K(\Phi)$ of K-automorphisms of (V_K, Φ_K). Moreover, given two k-objects (V, Φ) and (W, Ψ) as well as a K-isomorphism $g : (V_K, \Phi_K) \xrightarrow{\sim} (W_K, \Psi_K)$, one gets a map $G \to \mathrm{Aut}_K(\Phi)$ associating $a_\sigma = g^{-1} \circ \sigma(g)$ to $\sigma \in G$. The map a_σ satisfies the fundamental relation

$$a_{\sigma\tau} = a_\sigma \cdot \sigma(a_\tau) \quad \text{for all} \quad \sigma, \tau \in G. \tag{3}$$

Indeed, we compute

$$a_{\sigma\tau} = g^{-1} \circ \sigma(\tau(g)) = g^{-1} \circ \sigma(g) \circ \sigma(g^{-1}) \circ \sigma(\tau(g)) = a_\sigma \cdot \sigma(a_\tau).$$

Next, let $h : (V_K, \Phi_K) \xrightarrow{\sim} (W_K, \Psi_K)$ be another K-isomorphism, defining $b_\sigma := h^{-1} \circ \sigma(h)$ for $\sigma \in G$. Then a_σ and b_σ are related by

$$a_\sigma = c^{-1} b_\sigma \sigma(c), \tag{4}$$

where c is the K-automorphism $h^{-1} \circ g$. We abstract this in a general definition:

Definition 3.2. Let G be a group and A another (not necessarily commutative) group on which G acts on the left, i.e. there is a map $G \times A \to A$ sending a pair $(\sigma, a) \in G \times A$ to $\sigma(a) \in A$ so that the equalities $\sigma(ab) = \sigma(a)\sigma(b)$ and $\sigma\tau(a) = \sigma(\tau(a))$ hold for all $\sigma, \tau \in G$ and $a, b \in A$. Then a *1-cocycle* of G with values in A is a map $\sigma \mapsto a_\sigma$ from G to A satisfying the relation (3) above. Two 1-cocycles a_σ and b_σ are called *equivalent* or *cohomologous* if there exists $c \in A$ such that the relation (4) holds.

One defines the *first cohomology set* $H^1(G, A)$ of G with values in A as the quotient of the set of 1-cocycles by the equivalence relation (4). It is a *pointed set*, i.e. a set equipped with a distinguished element coming from the trivial cocycle $\sigma \mapsto 1$, where 1 is the identity element of A. We call this element the *base point*.

In our concrete situation, we see that the class $[a_\sigma]$ in $H^1(G, \mathrm{Aut}_K(\Phi))$ of the 1-cocycle a_σ associated with the K-isomorphism $g : (V_K, \Phi_K) \xrightarrow{\sim} (W_K, \Psi_K)$ depends only on (W, Ψ) but not on the map g. This enables us to state the main theorem of this section.

Theorem 3.3. *For a k-object (V, Φ) consider the pointed set $TF_K(V, \Phi)$ of twisted $(K|k)$-forms of (V, Φ), the base point being given by (V, Φ). Then the map $(W, \Psi) \to [a_\sigma]$ defined*

above yields a base point preserving bijection

$$TF_K(V,\Phi) \leftrightarrow H^1(G, \mathrm{Aut}_K(\Phi)).$$

Here is a crucial special case.

Example 3.4. (Hilbert's Theorem 90) Consider the case when V has dimension n over k and Φ is the trivial tensor. Then $\mathrm{Aut}_K(\Phi)$ is just the group $\mathrm{GL}_n(K)$ of invertible $n \times n$ matrices. On the other hand, two n-dimensional vector k-spaces that are isomorphic over K are isomorphic already over k, so we get:

$$H^1(G, \mathrm{GL}_n(K)) = \{1\}. \tag{5}$$

This statement is due to Speiser. The case $n = 1$ is usually called Hilbert's Theorem 90 in the literature, though Hilbert only considered the case when $K|k$ is a cyclic extension of degree n.

To prove Theorem 3.3, we construct an inverse to the map $(W, \Psi) \mapsto [a_\sigma]$. This is based on the following general construction.

Construction 3.5. Let A be a group equipped with a left action by another group G. Suppose further that X is a set on which both G and A act in a compatible way, i.e. we have $\sigma(a(x)) = (\sigma(a))(\sigma(x))$ for all $x \in X$, $a \in A$ and $\sigma \in G$. Assume finally given a 1-cocycle $\sigma \mapsto a_\sigma$ of G with values in A. Then we define the *twisted action of G on X by the cocycle a_σ* via the rule

$$(\sigma, x) \mapsto a_\sigma(\sigma(x)).$$

This is indeed a G-action, for the cocycle relation yields

$$a_{\sigma\tau}(\sigma\tau(x)) = a_\sigma \sigma(a_\tau)(\sigma\tau(x)) = a_\sigma \sigma(a_\tau \tau(x)).$$

If X is equipped with some algebraic structure (e.g. it is a group or a vector space), and G and A act on it by automorphisms, then the twisted action is also by automorphisms. The notation ${}_aX$ will mean X equipped with the twisted G-action by the cocycle a_σ.

Remark 3.6. Readers should be warned that the above construction can only be carried out on the level of cocycles and *not* on that of cohomology classes: equivalent cocycles give rise to different twisted actions in general. For instance, take $G = \mathrm{Gal}(K|k)$, $A = X = \mathrm{GL}_n(K)$, acting on itself by inner automorphisms. Then twisting the usual G-action on $\mathrm{GL}_n(K)$ by the trivial cocycle $\sigma \mapsto 1$ does not change anything, whereas if $\sigma \mapsto a_\sigma$ is a 1-cocycle with a_σ a noncentral element for some σ, then $a_\sigma^{-1}\sigma(x)a_\sigma \neq \sigma(x)$ for a noncentral x, so the twisted action is different. But a 1-cocycle $G \to \mathrm{GL}_n(K)$ is equivalent to the trivial cocycle by Example 3.4.

We now prove the special case considered in Example 3.4. The idea is to show that for a k-vector space V if we equip V_K with a twisted G-action and take G-invariants for the twisted action, we obtain a twisted form of V (which must be then k-isomorphic to V) The statement to be checked follows from:

Lemma 3.7 (Speiser)**.** *Let $K|k$ be a finite Galois extension with group G, and W a K-vector space equipped with a* semi-linear *G-action, i.e. a G-action satisfying*

$$\sigma(\lambda w) = \sigma(\lambda)\sigma(w) \quad \text{for all } \sigma \in G, w \in W \text{ and } \lambda \in K.$$

Then the natural map

$$\lambda : W^G \otimes_k K \to W$$

is an isomorphism, where the superscript G denotes invariants under G.

Lemma 3.8 (Dedekind)**.** *The elements of G are linearly independent in the K-vector space of functions $K \to K$.*

Proof. Let $\sigma_1, \dots, \sigma_n$ be the elements of G and assume there is a nontrivial relation $\sum_i b_i\sigma_i = 0$ with $b_i \in K$. Here we may assume the relation is of minimal length and $b_1, b_2 \neq 0$. Moreover, we may pick a nonzero $x \in K$ such that $\sigma_1(x) \neq \sigma_2(x)$. For every $y \in K$ we have $\sum_i b_i\sigma_i(xy) = \sum_i b_i\sigma_i(x)\sigma_i(y) = 0$. Thus $\sum_i b_i\sigma_i(x)\sigma_i = 0$; on the other hand $\sum_i b_i\sigma_1(x)\sigma_i = 0$ by multiplying the original relation by $\sigma_1(x)$. Since $\sigma_1(x) \neq \sigma_2(x)$ and $b_2 \neq 0$, it follows that $\sum_i b_i(\sigma_i(x) - \sigma_1(x))\sigma_i = 0$ is a shorter nontrivial relation, contradiction. □

Proof of Speiser's Lemma. For surjectivity we show that the elements of W^G generate W as a K-vector space. This will follow if we show that every K-linear function $\phi : W \to K$ whose restriction to W^G is 0 is in fact 0. With notation as above for fixed $w \in W$ the element $w_x := \sum_i \sigma_i(x)\sigma_i(w)$ lies in W^G for every $x \in K$, so $\phi(w_x) = 0$. But $\phi(w_x) = \sum_i \sigma_i(x)\phi(\sigma_i(w))$ for every x, so $\phi(\sigma_i(w)) = 0$ for all i by Dedekind's lemma. In particular, since one of the σ_i is the identity map, we get $\phi(w) = 0$ as required.

For injectivity, assume $w_1 \otimes b_1 + \cdots + w_r \otimes b_r \in W^G \otimes_k K$ is a nonzero element such that $b_1w_1 + \cdots b_rw_r = 0$ in W. We may assume that this is a relation of minimal length; in particular, the w_i are k-linearly independent in W^G. Furthermore, we may assume $b_1 = 1$ after multiplying by b_1^{-1}. Since the w_i are k-linearly independent, one of the b_i, say b_2, is not in K, so $\sigma(b_2) \neq b_2$ for some $\sigma \in G$. But then $w_1 + \sigma(b_2) +$

$\cdots \sigma(b_r)w_r = 0$ since $w_i \in W^G$ and $(\sigma(b_2)-b_2)w_2+\cdots+(\sigma(b_r)-b_r)w_r = 0$ is a shorter nontrivial relation, a contradiction. □

Proof of Theorem 3.3: As indicated above, we take a 1-cocycle a_σ representing some cohomology class in $H^1(G, \mathrm{Aut}_K(\Phi))$ and apply Construction 3.5 with $G = \mathrm{Gal}(K|k)$, $A = \mathrm{Aut}_K(\Phi)$ and $X = V_K$. As before, denote the invariant subspace by $({}_aV_K)^G$. Next observe that $\sigma(\Phi_K) = \Phi_K$ for all $\sigma \in G$ (as Φ_K comes from the k-tensor Φ) and also $a_\sigma(\Phi_K) = \Phi_K$ for all $\sigma \in G$ (as $a_\sigma \in \mathrm{Aut}_K(\Phi)$). Hence $a_\sigma\sigma(\Phi_K) = \Phi_K$ for all $\sigma \in G$, which means that Φ_K comes from a k-tensor on $({}_aV_K)^G$. Denoting this tensor by ${}_a\Phi$, we have defined a k-object $(({}_aV_K)^G, {}_a\Phi)$. Speiser's lemma yields an isomorphism $({}_aV_K)^G \otimes_k K \cong V_K$, and by construction this isomorphism identifies Ψ_K with Φ_K. Thus $(({}_aV_K)^G, {}_a\Phi)$ is indeed a twisted form of (V, Φ). If $a_\sigma = c^{-1}b_\sigma\sigma(c)$ with some 1-cocycle $\sigma \mapsto b_\sigma$ and $c \in \mathrm{Aut}_K(\Phi)$, we get from the definitions $({}_bV_K)^G = c(({}_aV_K)^G)$, which is a k-vector space isomorphic to $({}_aV_K)^G$. To sum up, we have a well-defined map $H^1(G, \mathrm{Aut}_K(\Phi)) \to TF_K(V, \Phi)$. The kind reader will check that this map is the inverse of the map $(W, \Psi) \mapsto [a_\sigma]$ of the theorem. □

Now we come to the classification of central simple algebras. First we recall a well-known fact about matrix rings:

Lemma 3.9. *Over a field K all automorphisms of the matrix ring $M_n(K)$ are inner, i.e. given by $M \mapsto CMC^{-1}$ for some invertible matrix C.*

Proof. Consider the minimal left ideal I_1 of $M_n(K)$ described in Example 1.5, and take an automorphism $\lambda \in \mathrm{Aut}(M_n(K))$. Give I_1 a new left $M_n(K)$-module structure by $(M, x) \mapsto \lambda(M)x$. We denote this $M_n(K)$-module by I_1^λ. Since I_1^λ is finite dimensional over K, it is a quotient of some finitely generated free $M_n(K)$-module $M_n(K)^m \cong I_1^{mn}$. As I_1 is a simple $M_n(K)$-module, the composite maps $I_1 \to I_1^{mn} \to I_1^\lambda$ must be trivial or injective for each component. Thus there is an injection $I_1 \to I_1^\lambda$ for some component which must then be an $M_n(K)$-module isomorphism $c : I_1 \xrightarrow{\sim} I_1^\lambda$ for dimension reasons. In particular, for every $M \in M_n(K)$ and $x \in I_1$ we have $c(M(x)) = M(c(x)) = \lambda(M)(c(x))$. Now consider c as a K-vector space automorphism of $I_1 \cong K^n$ corresponding to an invertible matrix C. We get $CM = \lambda(M)C$, so $\lambda(M) = CMC^{-1}$ as claimed. □

Corollary 3.10. *The automorphism group of $M_n(K)$ is the projective general linear group $\mathrm{PGL}_n(K)$.*

Proof. There is a natural homomorphism $\mathrm{GL}_n(K) \to \mathrm{Aut}(M_n(K))$ mapping $C \in \mathrm{GL}_n(K)$ to the automorphism $M \mapsto CMC^{-1}$. It is surjective by the lemma, and its kernel consists of the centre of $\mathrm{GL}_n(K)$, i.e. the subgroup of scalar matrices. □

Now take a finite Galois extension $K|k$ as before, and let $CSA_K(n)$ denote the set of k-isomorphism classes of central simple k-algebras of degree n split by K. We regard it as a pointed set, the base point being the class of the matrix algebra $M_n(k)$.

Theorem 3.11. *There is a base point preserving bijection*

$$CSA_K(n) \leftrightarrow H^1(G, \mathrm{PGL}_n(K)).$$

Proof. By Corollary 2.17 the central simple k-algebras of degree n are precisely the twisted forms of the matrix algebra $M_n(k)$. To see this, note that as explained in Example 3.1, an n^2-dimensional k-algebra can be considered as an n^2-dimensional k-vector space equipped with a tensor of type (1,2) satisfying the associativity condition. But on a twisted form of $M_n(k)$ the tensor defining the multiplication automatically satisfies the associativity condition. Hence Theorem 3.3 applies and yields a bijection of pointed sets $CSA_K(n) \leftrightarrow H^1(G, \mathrm{Aut}(M_n(K))$. The theorem now follows by Corollary 3.10. □

Our next goal is to classify all central simple k-algebras split by K by means of a single cohomology set. It should carry a product operation, since by virtue of Lemma 2.6 the tensor product induces a natural commutative and associative product operation

$$CSA_K(n) \times CSA_K(m) \to CSA_K(mn). \tag{6}$$

Via the bijection of Theorem 3.11 we obtain a corresponding product operation

$$H^1(G, \mathrm{PGL}_n(K)) \times H^1(G, \mathrm{PGL}_m(K)) \to H^1(G, \mathrm{PGL}_{nm}(K)) \tag{7}$$

on cohomology sets. To define this product directly, note that the map

$$\mathrm{End}_K(K^n) \otimes \mathrm{End}_K(K^m) \to \mathrm{End}_K(K^n \otimes K^m)$$

given by $(\phi, \psi) \mapsto \phi \otimes \psi$ restricts to a product operation

$$\mathrm{GL}_n(K) \times \mathrm{GL}_m(K) \to \mathrm{GL}_{nm}(K)$$

on invertible matrices which preserves scalar matrices, whence a product

$$\mathrm{PGL}_n(K) \times \mathrm{PGL}_m(K) \to \mathrm{PGL}_{nm}(K).$$

This induces a natural product on cocycles, whence the required product operation (7).

Next observe that for all $n, m > 0$ there are natural injective maps $\mathrm{GL}_n(K) \to \mathrm{GL}_{nm}(K)$ mapping a matrix $M \in \mathrm{GL}_n(K)$ to the block matrix given by m copies

of M placed along the diagonal and zeros elsewhere. As usual, these pass to the quotient modulo scalar matrices and finally induce maps

$$\lambda_{mn} : H^1(G, \mathrm{PGL}_m(K)) \to H^1(G, \mathrm{PGL}_{mn}(K))$$

on cohomology. Via the bijection of Theorem 3.11, the class of a central simple algebra A in $H^1(G, \mathrm{PGL}_m(K))$ is mapped to the class of $A \otimes_k M_n(k)$ by λ_{mn}.

Lemma 3.12. *The maps λ_{mn} are injective for all $m, n > 0$.*

Proof. Assume A and A' are central simple k-algebras with $A \otimes_k M_n(k) \cong A' \otimes_k M_n(k)$. By Wedderburn's theorem they are matrix algebras over division algebras D and D', respectively, hence so are $A \otimes_k M_n(k)$ and $A' \otimes_k M_n(k)$. But then $D \cong D'$ by the unicity statement in Wedderburn's theorem, so finally $A \cong A'$ by dimension reasons. □

Now define the set $H^1(G, \mathrm{PGL}_\infty)$ as the union for all n of the sets $H^1(G, \mathrm{PGL}_n(K))$ via the inclusion maps λ_{mn}, equipped with the product operation coming from (7) (which is manifestly compatible with the maps λ_{mn}). Also, observe that for a Galois extension $L|k$ containing K, the natural surjection $\mathrm{Gal}(L|k) \to \mathrm{Gal}(K|k)$ induces injective maps

$$H^1(\mathrm{Gal}(K|k), \mathrm{PGL}_n(K)) \to H^1(\mathrm{Gal}(L|k), \mathrm{PGL}_n(K))$$

for all n, and hence also injections

$$\iota_{LK} : H^1(\mathrm{Gal}(K|k), \mathrm{PGL}_\infty) \to H^1(\mathrm{Gal}(L|k), \mathrm{PGL}_\infty).$$

Fixing a separable closure k_s of k, we define $H^1(k, \mathrm{PGL}_\infty)$ as the union over all Galois extensions $K|k$ contained in k_s of the groups $H^1(\mathrm{Gal}(K|k), \mathrm{PGL}_\infty)$ via the inclusion maps ι_{LK}. The arguments above then yield:

Proposition 3.13. *The sets $H^1(G, \mathrm{PGL}_\infty)$ and $H^1(k, \mathrm{PGL}_\infty)$ equipped with the product operation coming from (7) are abelian groups, and there are natural group isomorphisms*

$$\mathrm{Br}(K|k) \cong H^1(G, \mathrm{PGL}_\infty) \quad \textit{and} \quad \mathrm{Br}(k) \cong H^1(k, \mathrm{PGL}_\infty).$$

Remark 3.14. The sets $H^1(G, \mathrm{PGL}_\infty)$ are not cohomology sets of G in the sense defined so far, but may be viewed as cohomology sets of G with values in the *direct limit* of the groups $\mathrm{PGL}_n(K)$ via the maps λ_{mn}. Still, this coefficient group is fairly complicated. In the next section we shall identify $\mathrm{Br}(K|k)$ with the second cohomology *group* of G with values in the multiplicative group $K^\times$, a group that is much easier to handle.

4. The cohomological Brauer group

In this section we first establish a formal proposition which, combined with the descent method, is a main tool in computations.

Proposition 4.1. *Let G be a group and*

$$1 \to A \to B \to C \to 1$$

an exact sequence of groups equipped with a G-action, the maps being G-homomorphisms. Then there is an exact sequence of pointed sets

$$1 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C).$$

By definition, an exact sequence of pointed sets is a sequence in which the kernel of each map equals the image of the previous one, the kernel being the subset of elements mapping to the base point. Note that, in contrast to the case of groups, a map with trivial kernel is *not* necessarily injective.

Proof. The only nonobvious points are the definition of the map $\delta : C^G \to H^1(G, A)$ and the exactness of the sequence at the third and fourth terms. To define δ, take an element $c \in C^G$ and lift it to an element $b \in B$ via the surjection $B \to C$. For all $\sigma \in G$ the element $b^{-1}\sigma(b)$ maps to 1 in C because $c = \sigma(c)$ by assumption, so it lies in A. Immediate calculations then show that the map $\sigma \mapsto b^{-1}\sigma(b)$ is a 1-cocycle and that modifying b by an element of A yields an equivalent cocycle, whence a well-defined map δ as required, sending elements coming from B^G to 1. The relation $\delta(c) = 1$ means by definition that $b^{-1}\sigma(b) = a^{-1}\sigma(a)$ for some $a \in A$, so c lifts to the G-invariant element ba^{-1} in B. This shows the exactness of the sequence at the third term, and the composition $C^G \to H^1(G, A) \to H^1(G, B)$ is trivial by construction. Finally, that a cocycle $\sigma \mapsto a_\sigma$ with values in A becomes trivial in $H^1(G, B)$ means that $a_\sigma = b^{-1}\sigma(b)$ for some $b \in B$, and modifying $\sigma \mapsto a_\sigma$ by an A-coboundary we may choose b so that its image c in C is fixed by G; moreover, the cohomology class of $\sigma \mapsto a_\sigma$ depends only on c. □

As a first application, we derive a basic theorem on central simple algebras.

Theorem 4.2. (Skolem-Noether) *All automorphisms of a central simple algebra are inner, i.e. given by conjugation by an invertible element.*

Proof. Let A be a central simple k-algebra of degree n and K a finite Galois splitting field of A. Denoting by $A^\times$ the subgroup of invertible elements of A and using Lemma 3.9 we get an exact sequence

$$1 \to K^\times \to (A \otimes_k K)^\times \to \mathrm{Aut}_K(A \otimes_k K) \to 1$$

of groups equipped with a $G = \mathrm{Gal}(K|k)$-action, where the second map maps an invertible element to the inner automorphism it defines. Proposition 4.1 then yields an exact sequence

$$1 \to k^\times \to A^\times \to \mathrm{Aut}_k(A) \to H^1(G, K^\times),$$

where the last term is trivial by Hilbert's Theorem 90. The theorem follows. □

We now come back to the situation of Proposition 4.1. In the case when A is contained in the centre of B (so in particular A is abelian), the exact sequence of the proposition can be extended on the right by the second cohomology group of A. Recall the formulas: A 2-*cocycle* of G with values in A (written multiplicatively) is a map $(\sigma, \tau) \mapsto a_{\sigma,\tau}$ from $G \times G$ to A satisfying the relation

$$\sigma(a_{\tau,\upsilon})a_{\sigma\tau,\upsilon}^{-1}a_{\sigma,\tau\upsilon}a_{\sigma,\tau}^{-1} = 1 \tag{8}$$

for all $\sigma, \tau, \upsilon \in G$. The 2-cocyle $a_{\sigma,\tau}a'^{-1}_{\sigma,\tau}$ is a *2-coboundary* if it is of the form $(\sigma, \tau) \mapsto a_\sigma\sigma(a_\tau)a_{\sigma\tau}^{-1}$ with some 1-cochain $\sigma \mapsto a_\sigma$ from G to A. The abelian group $H^2(G, A)$ is the quotient of the group of 2-cocycles is an abelian group by the subgroup of 2-coboundaries.

Proposition 4.3. *Let G be a group, and*

$$1 \to A \to B \to C \to 1$$

an exact sequence of groups equipped with a G-action, such that B and C are not necessarily commutative, but A is commutative and contained in the centre of B. Then there is an exact sequence of pointed sets

$$1 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to H^2(G, A).$$

Proof. The sequence was constructed until the penultimate term in Proposition 4.1. To define the map $\partial : H^1(G, C) \to H^2(G, A)$, take a 1-cocycle $\sigma \mapsto c_\sigma$ representing a class in $H^1(G, C)$, and lift each c_σ to an element $b_\sigma \in B$. The cocycle relation for $\sigma \mapsto c_\sigma$ implies that for all $\sigma, \tau \in G$ the element $b_\sigma\sigma(b_\tau)b_{\sigma\tau}^{-1}$ maps to 1 in C, hence comes from an element $a_{\sigma,\tau} \in A$. The function $(\sigma, \tau) \mapsto a_{\sigma,\tau}$ depends only on the class of $\sigma \mapsto c_\sigma$ in $H^1(G, C)$. Indeed, if we replace it by an equivalent cocycle $\sigma \mapsto c^{-1}c_\sigma\sigma(c)$, lifting c to $b \in B$ replaces $a_{\sigma\tau}$ by $(b^{-1}b_\sigma\sigma(b))(\sigma(b^{-1})\sigma(b_\tau)\sigma\tau(b))(\sigma\tau(b)^{-1}b_{\sigma,\tau}^{-1}b) = b^{-1}a_{\sigma,\tau}b$, which equals $a_{\sigma,\tau}$ because A is central in B. A straightforward calculation, which we leave to the readers, shows that $(\sigma, \tau) \mapsto a_{\sigma\tau}$ satisfies the 2-cocycle relation (8). Finally, replacing b_σ by another lifting $a_\sigma b_\sigma$ replaces $a_{\sigma,\tau}$ by $a_\sigma b_\sigma\sigma(a_\tau b_\tau)b_{\sigma\tau}^{-1}a_{\sigma\tau}^{-1} = a_\sigma\sigma(a_\tau)a_{\sigma\tau}^{-1}a_{\sigma,\tau}$, which has the same class in $H^2(G, A)$ (notice that we have used again that A is central in B). This defines the map ∂, and at the same time shows that it is trivial on the image of $H^1(G, B)$.

Finally, in the above notation, a class in $H^1(G,C)$ represented by $\sigma \mapsto c_\sigma$ is in the kernel of ∂ if the 2-cocycle $(\sigma,\tau) \mapsto b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$ equals a 2-coboundary $(\sigma,\tau) \mapsto a_\sigma \sigma(a_\tau) a_{\sigma\tau}^{-1}$. Replacing b_σ by the equivalent lifting $a_\sigma^{-1} b_\sigma$ we may assume $b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1} = 1$, which means that $\sigma \mapsto b_\sigma$ is a 1-cocycle representing a cohomology class in $H^1(G,B)$. □

Remark 4.4. The proposition does not hold in the above form when A is not contained in the centre of B. Instead, one has to work with twists of A.

We now apply Proposition 4.3 to the Brauer group. Let $K|k$ be a finite Galois extension of fields with group G, and m a positive integer. Applying the proposition to the exact sequence of G-groups

$$1 \to K^\times \to \mathrm{GL}_m(K) \to \mathrm{PGL}_m(K) \to 1$$

we get an exact sequence of pointed sets

$$H^1(G,\mathrm{GL}_m(K)) \longrightarrow H^1(G,\mathrm{PGL}_m(K)) \xrightarrow{\delta_m} H^2(G,K^\times). \tag{9}$$

Now recall the maps $\lambda_{mn} : H^1(G,\mathrm{PGL}_m(K)) \to H^1(G,\mathrm{PGL}_{mn}(K))$ introduced before Lemma 3.12.

Lemma 4.5. *The diagram*

$$\begin{array}{ccc} H^1(G,\mathrm{PGL}_m(K)) & \xrightarrow{\delta_m} & H^2(G,K^\times) \\ {\scriptstyle\lambda_{mn}}\downarrow & & \downarrow{\scriptstyle\mathrm{id}} \\ H^1(G,\mathrm{PGL}_{mn}(K)) & \xrightarrow{\delta_{mn}} & H^2(G,K^\times) \end{array}$$

commutes for all $m,n>0$.

Proof. A 1-cocycle $\sigma \mapsto c_\sigma$ representing a class in $H^1(G,\mathrm{PGL}_m(K))$ is mapped by δ_m to a 2-cocycle $a_{\sigma,\tau} = b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$ by the construction of the previous proof, where b_σ is given by some invertible matrix M_σ and $a_{\sigma,\tau}$ is the identity matrix I_m multiplied by some scalar $\mu_{\sigma,\tau} \in K^\times$. Performing the same construction for the image of $\sigma \mapsto c_\sigma$ by λ_{mn} means replacing M_σ by the block matrix with n copies of M_σ along the diagonal, which implies that the scalar matrix we obtain by taking the associated 2-cocycle is $\mu_{\sigma,\tau} I_{mn}$. □

By the lemma, taking the union of the pointed sets $H^1(G,\mathrm{PGL}_m(K))$ with respect to the maps λ_{mn} yields a map

$$\delta_\infty : H^1(G,\mathrm{PGL}_\infty) \to H^2(G,K^\times).$$

Equip the set $H^1(G, \mathrm{PGL}_\infty)$ with the group structure defined in Proposition 3.13. In Theorem 4.7 we shall prove that δ_∞ is an isomorphism. Here we establish a weaker statement which is already sufficient for a number of interesting applications.

Proposition 4.6. *The map δ_∞ is an injective group homomorphism.*

Proof. To show that δ_∞ preserves multiplication, take classes $c_m \in H^1(G, \mathrm{PGL}_m(K))$ and $c_n \in H^1(G, \mathrm{PGL}_n(K))$. With notations as in the previous proof, the classes $\delta_m(c_m)$ and $\delta_n(c_n)$ are represented by 2-cocycles of the form $(\sigma, \tau) \to \mu_{\sigma,\tau} I_m$ and $(\sigma, \tau) \to \nu_{\sigma,\tau} I_n$, respectively. From the fact that the product c_{mn} of $\lambda_{nm}(c_n)$ and $\lambda_{mn}(c_m)$ in $H^1(G, \mathrm{PGL}_{mn}(K))$ is induced by tensor product of linear maps we infer that $\delta_{mn}(c_{mn})$ is represented by a 2-cocycle mapping (σ, τ) to the tensor product of the linear maps given by multiplication by $\mu_{\sigma,\tau}$ and $\nu_{\sigma,\tau}$, respectively. But this tensor product is none but multiplication by $\mu_{\sigma,\tau}\nu_{\sigma,\tau}$, which was to be seen.

Once we know that δ_∞ is a group homomorphism, for injectivity it is enough to show that the map δ_m in exact sequence (9) has trivial kernel for all m. This follows from the exact sequence in view of the triviality of $H^1(G, \mathrm{GL}_m(K))$ (Example 3.4). □

We can finally prove:

Theorem 4.7. *The map δ_∞ induces an isomorphism*

$$H^1(G, \mathrm{PGL}_\infty) \xrightarrow{\sim} H^2(G, K^\times)$$

of abelian groups. Consequently, there is an isomorphism

$$\mathrm{Br}(K|k) \cong H^2(G, K^\times).$$

Before proving the theorem, let us recall a consequence of Galois theory. Let $K|k$ be a Galois extension as in the lemma, and consider two copies of K, the first one equipped with trivial G-action, and the second one with the action of G as the Galois group. Then the tensor product $K \otimes_k K$ (endowed with the G-action given by $\sigma(a \otimes b) \cong a \otimes \sigma(b)$) decomposes as a direct sum of copies of K:

$$K \otimes_k K \cong \bigoplus_{\sigma \in G} K e_\sigma, \tag{10}$$

where G acts on the right-hand side by permuting the basis elements e_σ. In other words, the tensor product $K \otimes_k K$ is isomorphic as a G-module to $K \otimes_{\mathbf{Z}} \mathbf{Z}[G]$.

To see this, write $K = k[x]/(f)$ with f some monic irreducible polynomial $f \in k[x]$, and choose a root α of f in K. As $K|k$ is Galois, f splits in $K[x]$ as a product of linear terms of the form $(x - \sigma(\alpha))$ for $\sigma \in G$. Thus using a special case of the Chinese Remainder Theorem for rings (which is easy to prove directly) we get

$$K \otimes_k K \cong K[x]/(f) \cong K[x]/(\prod_{\sigma \in G} (x - \sigma(\alpha)) \cong \bigoplus_{\sigma \in G} K[x]/(x - \sigma(\alpha)),$$

whence a decomposition of the required form.

Proof. The second statement follows from the first in view of Proposition 3.13, and for the first statement it remains to prove surjectivity of the map δ_∞. We show much more, namely that the map δ_n is surjective, where n is the order of G. For this, consider $K \otimes_k K$ as a K-vector space. Multiplication by an invertible element of $K \otimes_k K$ is a K-linear automorphism $K \otimes_k K \to K \otimes_k K$. In this way we get a group homomorphism $(K \otimes_k K)^\times \to \mathrm{GL}_n(K)$ which we may insert into a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times & \longrightarrow & (K \otimes_k K)^\times & \longrightarrow & (K \otimes_k K)^\times / K^\times & \longrightarrow & 1 \\ & & \mathrm{id}\downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & K^\times & \longrightarrow & \mathrm{GL}_n(K) & \longrightarrow & \mathrm{PGL}_n(K) & \longrightarrow & 1 \end{array}$$

where all maps are compatible with the action of G if we make G act on $K \otimes_k K$ via the right factor and on the other terms by the standard action. Hence by taking cohomology we get a commutative diagram

$$\begin{array}{ccccc} H^1(G, (K \otimes_k K)^\times / K^\times) & \xrightarrow{\alpha} & H^2(G, K^\times) & \longrightarrow & H^2(G, (K \otimes_k K)^\times) \\ \downarrow & & \mathrm{id}\downarrow & & \\ H^1(G, \mathrm{PGL}_n(K)) & \xrightarrow{\delta_n} & H^2(G, K^\times) & & \end{array}$$

where the upper row is exact. Now the discussion before the proof implies that $(K \otimes_k K)^\times$ is isomorphic to the G-module $K^\times \otimes_{\mathbf{Z}} \mathbf{Z}[G]$, because the invertible elements in $\bigoplus Ke_i$ are exactly those with coefficients in $K^\times$. Now since G is finite, there is a non-canonical isomorphism of G-modules $K^\times \otimes_{\mathbf{Z}} \mathbf{Z}[G] \cong \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}[G], K^\times)$. In other words, the G-module $(K \otimes_k K)^\times$ is co-induced, hence the group $H^2(G, (K \otimes_k K)^\times)$ is trivial. This yields the surjectivity of the map α in the diagram, and hence also that of δ_n by commutativity of the diagram. □

Corollary 4.8. *Let $K|k$ be a Galois extension of degree n. Then each element of the relative Brauer group $\mathrm{Br}(K|k)$ has order dividing n.*

Consequently, the full Brauer group $\mathrm{Br}(k)$ is a torsion abelian group.

Proof. This follows from the theorem together with the fact that $H^2(G, A)$ for any G-module A is annihilated by the order of G (consequence of a restriction-corestriction argument). □

In the case of a finite cyclic Galois extension the theorem gives a means to compute the relative Brauer group. Recall that for a finite Galois extension $K|k$ with

group G the *norm map* $N_{K|k} : K \to k$ sends $a \in K$ to $\prod_{\sigma \in G} \sigma(a)$; it restricts to a homomorphism on multiplicative groups.

Corollary 4.9. *For a finite cyclic Galois extension $K|k$ there is an isomorphism*

$$\mathrm{Br}(K|k) \cong k^\times / N_{K|k}(K^\times).$$

This follows from the theorem together with the following general lemma in group cohomology.

Lemma 4.10. *Let G be a finite cyclic group of order n, generated by an element σ. For a G-module A, define maps $N : A \to A$ and $\sigma - 1 : A \to A$ by*

$$N : a \mapsto \sum_{i=0}^{n-1} \sigma^i a \quad \text{and} \quad \sigma - 1 : a \mapsto \sigma a - a$$

and put ${}_N A := \ker(N)$. With these notations we have

$$H^0(G, A) = A^G,\ H^{2i+1}(G, A) = {}_N A/(\sigma - 1)A \text{ and } H^{2i+2}(G, A) = A^G/NA \tag{11}$$

for $i > 0$.

Proof. Consider the maps N and $\sigma - 1$ for $A = \mathbf{Z}[G]$. One checks easily that in this case $\ker(N) = \mathrm{Im}\,(\sigma - 1)$ and $\mathrm{Im}\,(N) = \ker(\sigma - 1)$. Hence we obtain a free resolution

$$\cdots \xrightarrow{N} \mathbf{Z}[G] \xrightarrow{\sigma - 1} \mathbf{Z}[G] \xrightarrow{N} \mathbf{Z}[G] \xrightarrow{\sigma - 1} \mathbf{Z}[G] \to \mathbf{Z} \to 0,$$

the last map being induced by $\sigma \mapsto 1$. Computing the groups $H^j(G, A)$ using this free resolution yields the formulas of the lemma. □

Remark 4.11. If $K|k$ is a finite Galois extension with cyclic Galois group G as above, the lemma applied with $A = K^\times$ also shows $H^1(G, K^\times) = {}_N K^\times/(\sigma - 1)K^\times$. The first group is trivial by Hilbert's Theorem 90 and we obtain the original form of the theorem proven by Hilbert: *In a cyclic field extension $K|k$ with $\mathrm{Gal}(K|k) =< \sigma >$ each element of norm 1 is of the form $\sigma(c)c^{-1}$ with some $c \in K$.*

Finally, we can use Corollary 4.9 to give the first concrete examples of fields with nontrivial Brauer group.

Example 4.12. For the field $\mathbf{R}$ of real numbers we have

$$\mathrm{Br}(\mathbf{R}) \cong \mathbf{R}^\times / N_{\mathbf{C}|\mathbf{R}}(\mathbf{C}^\times) \cong \mathbf{Z}/2\mathbf{Z}.$$

Indeed, the norm map $N_{\mathbf{C}|\mathbf{R}} : \mathbf{C}^\times \to \mathbf{R}^\times$ sends $a + bi$ to $a^2 + b^2$, whence $N_{\mathbf{C}|\mathbf{R}}(\mathbf{C}^\times)$ equals the positive real numbers. Consequently, there is only one nontrivial Brauer

class which must be that of the Hamilton quaternions. This proves a classical theorem of Frobenius: *The only finite-dimensional division algebras over* $\mathbf{R}$ *are* $\mathbf{R}$, $\mathbf{C}$ *and the Hamilton quaternions.*

Example 4.13. The Brauer group of a finite field is trivial. To see this, we have to show $\mathrm{Br}(\mathbf{F}_{q^r}|\mathbf{F}_q) = 0$ for all q and r, where $\mathbf{F}_{q^r}$ is the finite field with q^r elements. By Corollary 4.9 this amounts to showing surjectivity of the norm map $N := N_{\mathbf{F}_{q^r}|\mathbf{F}_q}$.

Since the extension $\mathbf{F}_{q^r}|\mathbf{F}_q$ is known to be cyclic with generator $\sigma : a \mapsto a^q$, the norm map N equals $a \mapsto a^{\frac{q^r-1}{q-1}}$. On the other hand, the multiplicative group $\mathbf{F}_{q^r}^\times$ is also cyclic, so if ω is a generator, then $N(\omega) \in \mathbf{F}_q^\times$. It follows that $N(\omega), N(\omega^2), \ldots, N(\omega^{q-1})$ give the elements of $\mathbf{F}_q^\times$.

We have proven another theorem of Wedderburn: *Over a finite field every finite-dimensional division algebra is commutative.*

5. Index and period

In this section we use the cohomological theory of the Brauer group to derive basic results of Brauer concerning two important invariants for central simple algebras. By Example 4.13 we can assume throughout that the base field k is infinite, otherwise the discussion to follow is vacuous.

The first of the announced invariants is the following.

Definition 5.1. Let A be a central simple algebra over a field k. The *index* $\mathrm{ind}_k(A)$ of A over k is defined to be the degree of D over k, where D is the division algebra for which $A \cong M_n(D)$ according to Wedderburn's theorem. We shall drop the subscript k from the notation when clear from the context.

Remarks 5.2.

(1) For a division algebra index and degree are one and the same thing.
(2) The index of a central simple k-algebra A depends only on the class of A in the Brauer group $\mathrm{Br}(k)$. Indeed, this class depends only on the division algebra D associated with A by Wedderburn's theorem, and the index is by definition an invariant of D.
(3) We have $\mathrm{ind}\,(A) = 1$ if and only if A is split.

Proposition 5.3. *Let A be a central simple k-algebra. The index $\mathrm{ind}\,(A)$ is the greatest common divisor of the degrees of finite separable field extensions $K|k$ that split A.*

For the proof we need the following refinement of Theorem 4.7.

Proposition 5.4. *Let $K|k$ be a separable field extension of degree n. Let $\widetilde{K}$ be the Galois closure of K, and denote the Galois groups $\mathrm{Gal}(\widetilde{K}|k)$ and $\mathrm{Gal}(\widetilde{K}|K)$ by G and H, respectively.*

The boundary map $\delta_n :\ H^1(G, \mathrm{PGL}_n(\widetilde{K})) \to \mathrm{Br}(\widetilde{K}|k)$ *induces a bijection*

$$\ker(H^1(G, \mathrm{PGL}_n(\widetilde{K})) \to H^1(H, \mathrm{PGL}_n(\widetilde{K}))) \xrightarrow{\sim} \mathrm{Br}(K|k).$$

The proof uses a lemma from Galois theory.

Lemma 5.5. *Making* G *act on the tensor product* $K \otimes_k \widetilde{K}$ *via the second factor, we have an isomorphism of* G*–modules*

$$(K \otimes_k \widetilde{K})^\times \cong M_H^G(\widetilde{K}^\times).$$

Proof. According to the theorem of the primitive element, we may write $K = k(\alpha)$ for some $\alpha \in K$ with minimal polynomial $f \in k[x]$, so that $\widetilde{K}$ is the splitting field of f. By Galois theory, if $1 = \sigma_1, \ldots, \sigma_n$ is a system of left coset representatives for H in G, the roots of f in K are exactly the $\sigma_i(\alpha)$ for $1 \leq i \leq n$. So we get, just like before the proof of Theorem 4.7, a chain of isomorphisms

$$K \otimes_k \widetilde{K} \cong \widetilde{K}[x]/\prod_{i=1}^{n}(x - \sigma_i(\alpha)) \cong \mathrm{Hom}_H(\mathbf{Z}[G], \widetilde{K}) = M_H^G(\widetilde{K}).$$

The lemma follows by restricting to invertible elements. □

Proof of Proposition 5.4: We have already shown in the proof of Theorem 4.7 the injectivity of δ_n (even of δ_∞), so it suffices to see surjectivity. With the notations of the lemma above, consider the short exact sequence of G-modules

$$1 \to \widetilde{K}^\times \to (K \otimes_k \widetilde{K})^\times \to (K \otimes_k \widetilde{K})^\times/\widetilde{K}^\times \to 1,$$

where G acts on $K \otimes_k \widetilde{K}$ via the second factor. Part of the associated long exact sequence reads

$$H^1(G, (K \otimes_k \widetilde{K})^\times/\widetilde{K}^\times) \to H^2(G, \widetilde{K}^\times) \to H^2(G, (K \otimes_k \widetilde{K})^\times). \tag{12}$$

Using the previous lemma, Shapiro's lemma and Theorem 4.7, we get a chain of isomorphisms

$$H^2(G, (K \otimes_k \widetilde{K})^\times) \cong H^2(G, M_H^G(\widetilde{K})) \cong H^2(H, \widetilde{K}) \cong \mathrm{Br}(\widetilde{K}|K).$$

We also have $H^2(G, \widetilde{K}^\times) \cong \mathrm{Br}(\widetilde{K}|k)$, so all in all we get from exact sequence (12) a surjection

$$\widetilde{\alpha} :\ H^1(G, (K \otimes_k \widetilde{K})^\times/\widetilde{K}^\times) \to \mathrm{Br}(K|k)$$

On the other hand, the choice of a k-basis of K provides an embedding $K \hookrightarrow M_n(k)$, whence a G-equivariant map $K \otimes_k \widetilde{K} \to M_n(\widetilde{K})$, and finally a map $(K \otimes_k \widetilde{K})^\times \to$

$\mathrm{GL}_n(\widetilde{K})$. Arguing as in the proof of Theorem 4.7, we get a commutative diagram:

$$\begin{array}{ccc} H^1(G,(K\otimes_k\widetilde{K})^\times/K^\times) & \xrightarrow{\widetilde{\alpha}} & H^2(G,\widetilde{K}^\times) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ H^1(G,\mathrm{PGL}_n(\widetilde{K})) & \xrightarrow{\delta_n} & H^2(G,\widetilde{K}^\times) \end{array}$$

Therefore by the surjectivity of $\widetilde{\alpha}$ each element of $\mathrm{Br}(K|k) \subset H^2(G,\widetilde{K}^\times)$ comes from some element in $H^1(G,\mathrm{PGL}_n(\widetilde{K}))$. By the injectivity of δ_n and its obvious compatibility with restriction maps, this element restricts to 1 in $H^1(H,\mathrm{PGL}_n(\widetilde{K}))$, as required. □

Proof of Proposition 5.3. In view of Theorem 2.12 it is enough to show that if a finite separable extension $K|k$ of degree n splits A, then $\mathrm{ind}\,(A)$ divides n. For such a K, the class of A in $\mathrm{Br}(K|k)$ comes from a class in $H^1(G,\mathrm{PGL}_n(\widetilde{K}))$ according to Proposition 5.4. By Theorem 3.11 this class is also represented by some central simple k-algebra B of degree n, hence of index dividing n. But $\mathrm{ind}\,(A)=\mathrm{ind}\,(B)$ by Remark 5.2 (2). □

Combining with Theorem 2.12 we get:

Corollary 5.6. *The index* $\mathrm{ind}\,(A)$ *is the smallest among the degrees of finite separable field extensions* $K|k$ *that split* A*.*

Here is another useful corollary.

Corollary 5.7. *Let* $K|k$ *be a finite separable field extension.*

(1) *We have the divisibility relations*

$$\mathrm{ind}_K(A\otimes_k K) \mid \mathrm{ind}_k(A) \mid [K:k]\,\mathrm{ind}_K(A\otimes_k K).$$

(2) *If* $\mathrm{ind}_k(A)$ *is prime to* $[K:k]$*, then* $\mathrm{ind}_k(A)=\mathrm{ind}_K(A\otimes_k K)$*. In particular, if* A *is a division algebra, then so is* $A\otimes_k K$*.*

Proof. It is enough to prove the first statement. The divisibility relation $\mathrm{ind}_K(A\otimes_k K) \mid \mathrm{ind}_k(A)$ is immediate from the proposition. For the second one, use Theorem 2.12 to find a finite separable field extension $K'|K$ splitting $A\otimes_k K$ with $[K':K]=\mathrm{ind}_K(A\otimes_k K)$. Then K' is also a splitting field of A, so Proposition 5.3 shows $\mathrm{ind}_k(A) \mid [K':k]=\mathrm{ind}_K(A\otimes_k K)[K:k]$. □

Now we come to the second main invariant.

Definition 5.8. The *period* (or *exponent*) of a central simple k-algebra A is the order of its class in $\mathrm{Br}(k)$. We denote it by $\mathrm{per}\,(A)$.

The basic relations between the period and the index are the following.

Proposition 5.9. (Brauer) *Let A be a central simple k-algebra.*

(1) *The period* $\mathrm{per}\,(A)$ *divides the index* $\mathrm{ind}\,(A)$.
(2) *The period* $\mathrm{per}\,(A)$ *and the index* $\mathrm{ind}\,(A)$ *have the same prime factors.*

For the proof of the second statement we shall need the following lemma.

Lemma 5.10. *Let p be a prime number not dividing* $\mathrm{per}\,(A)$. *Then A is split by a finite separable extension $K|k$ of degree prime to p.*

Proof. Let $L|k$ be a finite Galois extension that splits A, let P be a p-Sylow subroup of $\mathrm{Gal}(L|k)$ and K its fixed field. Then $\mathrm{Br}(L|K) \cong H^2(P, L^\times)$ is a p-primary torsion group by Corollary 4.8, so the assumption implies that the image of $[A]$ by the restriction map $\mathrm{Br}(L|k) \to \mathrm{Br}(L|K)$ is trivial. This means that A is split by K. □

Proof of Proposition 5.9: According to Theorem 2.12, the algebra A is split by a separable extension $K|k$ of degree $\mathrm{ind}\,(A)$ over A. If $\widetilde{K}$ is a Galois closure of K, Proposition 5.4 implies that the class $[A]$ of A in $\mathrm{Br}(\widetilde{K}|k)$ is annihilated by the restriction map $\mathrm{Br}(\widetilde{K}|k) \to \mathrm{Br}(\widetilde{K}|K)$. Composing with the corestriction $\mathrm{Br}(\widetilde{K}|k) \to \mathrm{Br}(\widetilde{K}|K)$ and using that $\mathrm{Cor} \circ \mathrm{Res} = [K : k]$, we get that $[A]$ is annihilated by multiplication by $[K : k] = \mathrm{ind}\,(A)$, whence the first statement. For the second statement, let p be a prime number that does not divide $\mathrm{per}\,(A)$. By the lemma above, there exists a finite separable splitting field $K|k$ with $[K : k]$ prime to p. Hence by Proposition 5.3, the index $\mathrm{ind}\,(A)$ is also prime to p. □

As an application of the above, we finally prove the following decomposition result.

Proposition 5.11. (Brauer) *Let D be a central division algebra over k. Consider the primary decomposition*

$$\mathrm{ind}\,(D) = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}.$$

Then we may find central division algebras D_i $(i = 1, .., r)$ such that

$$D \cong D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_r$$

and $\mathrm{ind}\,(D_i) = p_i^{m_i}$ *for $i = 1, .., r$. Moreover, the D_i are uniquely determined up to isomorphism.*

Proof. The Brauer group is torsion (Corollary 4.8), so it splits into p-primary components:

$$\mathrm{Br}(k) = \bigoplus_p \mathrm{Br}(k)\{p\}.$$

In this decomposition the class of D decomposes as a sum

$$[D] = [D_1] + [D_2] + \cdots + [D_r]$$

where the D_i are division algebras with $[D_i] \in \mathrm{Br}(k)\{p_i\}$ for some primes p_i. By Proposition 5.9 (2) the index of each D_i is a power of p_i. The tensor product $A = D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_r$ has degree $\prod_i \mathrm{ind}\,(D_i)$ over k and its index equals that of D by Remark 5.2 (2), so $\mathrm{ind}\,D$ divides $\prod_i \mathrm{ind}\,(D_i)$. A repeated application of Theorem 2.12 shows that for fixed i one may find a finite separable extension $K_i|k$ of degree prime to p_i that splits all the D_j for $j \neq i$. Then $D \otimes_k K_i$ and $D_i \otimes_k K_i$ have the same class in $\mathrm{Br}(K_i)$, and thus $\mathrm{ind}_{K_i}(D_i \otimes_k K_i) \mid \mathrm{ind}\,(D)$ by Corollary 5.7 (1). The algebras $D_i \otimes_k K_i$ are still division algebras of index $\mathrm{ind}\,(D_i)$ over K_i by Corollary 5.7 (2). To sum up, we have proven that $\mathrm{ind}\,(D_i)$ divides $\mathrm{ind}\,(D)$ for all i, so we conclude that $\mathrm{ind}\,(D) = \prod_i \mathrm{ind}\,(D_i)$. The k-algebras D and $D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_r$ thus have the same Brauer class and same dimension, hence they are isomorphic as claimed. The unicity of the D_i holds for the same reason. □

6. Central simple algebras over complete discretely valued fields

In this section K denotes a field complete with respect to a discrete valuation, with perfect residue field κ. Our first goal is to prove:

Theorem 6.1. *Every central simple algebra A over K is split by a finite unramified extension of K.*

The bulk of the proof of the theorem is contained in the following proposition.

Proposition 6.2. *Every central division algebra D of degree $d > 1$ over K contains a K-subalgebra L that is an unramified field extension of K of degree > 1.*

We prove the proposition following the method of Serre [2], §XII.2. The key tool is the extension of the valuation on K to D. By definition, a discrete valuation on a division algebra D is a map $w : D \to \mathbf{Z} \cup \{\infty\}$ satisfying the same properties as in the commutative case. The elements satisfying $w(x) \geq 0$ form a subring $A_w \subset D$ in which the set M_w of elements with $w(x) > 0$ is a two-sided ideal. Fixing an element $\pi \in D$ such that $w(\pi)$ is the positive generator of the subgroup $w(D \setminus \{0\}) \subset \mathbf{Z}$, we may write each $m \in M_w$ in the form $m = b\pi$ with $b \in A_w$.

To extend discrete valuations from K to D we need the notion of reduced norms.

Construction 6.3. Let A be a central simple k-algebra of degree n. Take a finite Galois splitting field $K|k$ with group G, and choose a K-isomorphism $\phi : M_n(K) \xrightarrow{\sim}$

$A \otimes_k K$. Recall that the isomorphism ϕ is not compatible with the action of G. However, if we twist the usual action of G on $M_n(K)$ by the 1-cocycle $\sigma \mapsto a_\sigma$ with $a_\sigma = \phi^{-1} \circ \sigma(\phi)$ associated with A by the descent construction, then we get an isomorphism ${}_aM_n(K) \tilde{\to} A \otimes_k K$ that is already G-equivariant, whence an isomorphism $({}_aM_n(K))^G \cong A$.

Now consider the determinant map $\det : M_n(K) \to K$. For all $\sigma \in G$, lifting a_σ to an invertible matrix $C_\sigma \in \mathrm{GL}_n(K)$ we get

$$\det(C_\sigma \sigma(M) C_\sigma^{-1}) = \det(\sigma(M)) = \sigma(\det(M)) \tag{13}$$

by multiplicativity of the determinant and its compatibility with the usual G-action. Bearing in mind that the twisted G-action on ${}_aM_n(K)$ is given by $(\sigma, M) \to a_\sigma \sigma(M) a_\sigma^{-1}$, this implies that the map $\det : {}_aM_n(K) \to K$ is compatible with the action of G. So by taking G-invariants and using the isomorphism above we get a map $\mathrm{Nrd} : A \to k$, called the *reduced norm map*. On the subgroup $A^\times$ of invertible elements of A it restricts to a group homomorphism $\mathrm{Nrd} : A^\times \to k^\times$.

The above construction does not depend on the choice of ϕ, for changing ϕ amounts to replacing a_σ by an equivalent cocycle, i.e. replacing the matrix C_σ above by some $D^{-1} C_\sigma \sigma(D)$, which does not affect the expression in (13). The construction does not depend on the choice of K either, as one sees by embedding two Galois splitting fields K, L into a bigger Galois extension $M|k$.

The reduced norm map is a generalization of the norm map for quaternion algebras. Just like the quaternion norm, it enjoys the following property:

Proposition 6.4. *In a central simple k-algebra A an element $a \in A$ is invertible if and only if $\mathrm{Nrd}\,(a) \neq 0$. Hence A is a division algebra if and only if Nrd restricts to a nowhere vanishing map on $A \setminus 0$.*

Proof. If a is invertible, it corresponds to an invertible matrix via any isomorphism $\phi : A \otimes_K K \cong M_n(K)$, which thus has nonzero determinant. For the converse, consider ϕ as above and assume an element $a \in A$ maps to a matrix with nonzero determinant. It thus has an inverse $b \in M_n(K)$. Now in any ring the multiplicative inverse of an element is unique (indeed, if b' is another inverse, one has $b = bab' = b'$), so for an automorphism $\sigma_A \in \mathrm{Aut}_k(A \otimes_k K)$ coming from the action of an element $\sigma \in \mathrm{Gal}(K|k)$ on K we have $\sigma_A(b) = b$. As A is the set of fixed elements of all the σ_A, this implies $b \in A$. □

Now recall that given a finite dimensional k-algebra A, the *norm* of an element $a \in A$ are defined as follows: one considers the k-linear mapping $L_a : A \to A$ given by $L_a(x) = ax$ and puts $N_{A|k}(a) := \det(L_a)$.

Proposition 6.5. *If A is a central simple k-algebra of degree n, then $N_{A|k} = (\mathrm{Nrd}_A)^n$.*

Proof. We may assume, up to passing to a splitting field of A, that $A = M_n(k)$. The required formulae then follow from the fact that for $M \in M_n(k)$, the matrix of the multiplication-by-M map L_M with respect to the standard basis of $M_n(k)$ is the block diagonal matrix $\mathrm{diag}(M, \dots, M)$. □

Lemma 6.6. *If D and K are as in the proposition, the discrete valuation v of K extends to a unique discrete valuation on D, given by the formula*

$$w = \frac{1}{d}\, v \circ \mathrm{Nrd}_D.$$

Moreover, D is complete with respect to w.

Proof. We first show that if $L|K$ is a field extension contained in D, then for $x \in L$ we have

$$\frac{1}{d}\, v(\mathrm{Nrd}_D(x)) = \frac{1}{[L:K]}\, v(N_{L|K}(x)). \tag{14}$$

Indeed, Proposition 6.5 gives $N_{D|K} = (\mathrm{Nrd}_D)^d$. On the other hand, viewing D as an L-vector space of dimension $d^2/[L:K]$, we have

$$N_{D|K}(x) = N_{L|K}(x)^{d^2/[L:K]}$$

for $x \in L$. It follows that we have an equality

$$\mathrm{Nrd}_D(x) = \omega\, N_{L|K}(x)^{d/[L:K]}$$

in K with some d-th root of unity ω, whence formula (14) follows after applying v.

Applying formula (14) with $L = K$ gives $w|_K = v$. Applying it to the subfields $K(x) \subset D$ generated by each $x \in D$ and comparing with the description of the unique extension of v to finite field extensions implies the uniqueness of the extension to D. Next, we check that w as defined above is a discrete valuation. The implication $w(x) = \infty \Rightarrow x = 0$ follows from Proposition 6.4, and the formula $w(xy) = w(x) + w(y)$ from the multiplicativity of the reduced norm. The property $w(x+y) \geq \min(w(x), w(y))$ reduces to $w(1 + x^{-1}y) \geq \min(1, w(x^{-1}y))$ after subtracting $w(x)$. The latter can be checked in the field $L = K(x^{-1}y)$ where it holds because, as remarked above, formula (14) implies that $w|_L$ is a multiple of the unique extension of v to L. Finally, the completeness of D with respect to the w-adic topology is proven as in the commutative case. □

Proof of Proposition 6.2. Extend the valuation v of K to a discrete valuation w of D as in the lemma above. If the statement of the proposition does not hold, then for each finite field extension $L|K$ contained in D the valuation $w|_L$ has residue field equal

to that of v. In particular, this holds for the subfield $L = K(b)$ generated by any $b \in A_w$. Fixing b, we thus find a_0 in the ring of integers A_v of K with $b - a_0 \in M_w$. Fixing moreover a generator π as after the statement of the proposition we may write

$$b = a_0 + b_1\pi$$

with some $b_1 \in A_w$. Repeating the procedure with b_1 in place of b and continuing in the same way, we construct inductively for each $N > 0$ elements $a_N \in A_v$ and $b_N \in A_w$ satisfying

$$b = \sum_{i=0}^{N-1} a_i\pi^i + b_N\pi^N.$$

We infer that b is in the closure of the subfield $K(\pi) \subset D$ for the w-adic topology on D. But $K(\pi)$ is closed in D (this holds for any linear subspace in a finite-dimensional normed vector space over a complete valued field and is easily checked by taking coordinates), whence $b \in K(\pi)$. Since b was arbitrary here and for every $x \in D$ we have $x\pi^m \in A_w$ for m large enough, we conclude $D \subset K(\pi)$, contradicting the assumption that the centre of D is K. □

Proof of Theorem 6.1. We use induction on the index d of A, the case $d = 1$ being obvious. Using Wedderburn's theorem we may assume that A is a division algebra of degree d. Applying Proposition 6.2, we find a nontrivial unramified field extension $L|K$ that embeds in A over K. The L-algebra $A \otimes_K L$ is not a division algebra because it contains $L \otimes_K L$ which is a product of copies of L. Thus $\mathrm{ind}\,(A \otimes_K L) < \mathrm{ind}\,(A) = d$, and therefore $A \otimes_K L$ splits over an unramified extension $M|L$ by the inductive assumption. But $M|K$ is again an unramified extension, which concludes the proof. □

Now denote by K_{nr} the maximal unramified extension of K, i.e. the compositum of all finite unramified extensions of K inside a fixed separable closure. The theorem then implies:

Corollary 6.7. *We have* $\mathrm{Br}(K) = \mathrm{Br}(K_{nr}|K)$.

So we are left to study the relative Brauer group $\mathrm{Br}(K_{nr}|K)$. To do so, let $L|K$ be a finite *unramified* Galois extension with group G. Denoting by U_L the multiplicative group of units in L, the valuation v of L defines an exact sequence of G-modules

$$1 \to U_L \to L^\times \xrightarrow{v} \mathbf{Z} \to 0 \tag{15}$$

which is split by the map $\mathbf{Z} \to L^\times$ sending 1 to a local parameter π of v. (Note that $\pi \in K$ and hence is G-invariant because $L|K$ is unramified.) Therefore we have a

split exact sequence of cohomology groups

$$0 \to H^2(G, U_L) \to H^2(G, L^\times) \to H^2(G, \mathbf{Z}) \to 0.$$

Next note that $H^i(G, \mathbf{Q}) = 0$ for all $i > 0$: indeed, if G has order n, then on the one hand $n\, H^i(G, \mathbf{Q}) = 0$, on the other hand, since the multiplication-by-n map $\mathbf{Q} \xrightarrow{n} \mathbf{Q}$ is an isomorphism, so is $H^i(G, \mathbf{Q}) \xrightarrow{n} H^i(G, \mathbf{Q})$. So we can use the exact sequence

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$$

to obtain isomorphisms $H^2(G, \mathbf{Z}) \cong H^1(G, \mathbf{Q}/\mathbf{Z}) \cong \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$ and we may rewrite the above sequence as

$$0 \to H^2(G, U_L) \to H^2(G, L^\times) \to \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z}) \to 0.$$

Now we study the group on the left.

Proposition 6.8. *Let $L|K$ be a finite unramified Galois extension with group G and let λ be the residue field of L. The natural reduction map $U_L \to \lambda^\times$ induces isomorphisms*

$$H^2(G, U_L) \cong H^2(G, \lambda^\times).$$

Therefore we have a split exact sequence

$$0 \to \mathrm{Br}(\lambda|\kappa) \to \mathrm{Br}(L|K) \to \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z}) \to 0.$$

For the proof we need a formal lemma.

Lemma 6.9. *Let G be a finite group, and (A_j, ϕ_j) an inverse system of G-modules indexed by the set $\mathbf{Z}_+$ of positive integers, with surjective transition maps ϕ_j. If $i > 0$ is an integer such that $H^i(G, A_1) = H^i(G, \ker(\phi_j)) = 0$ for all j, then $H^i(G, \varprojlim A_j)$=0.*

Proof. Choose a projective resolution $P_\bullet$ of $\mathbf{Z}$, and represent an element of $H^i(G, \varprojlim A_j)$ by a collection of homomorphisms $\lambda_j : P_i \to A_j$ each of which are mapped to 0 by δ_*^i. By induction on j we construct $\mu \in \mathrm{Hom}(P_{i-1}, \varprojlim A_j)$ represented by homomorphisms $\mu_j : P_{i-1} \to A_j$ with $\delta_*^{i-1}(\mu_j) = \lambda_j$. The existence of μ_1 follows from $H^i(G, A_1) = 0$. Assuming μ_j has been constructed, lift it to a homomorphism $\mu'_{j+1} : P_{i-1} \to A_{j+1}$ using the surjectivity of $\phi_j : A_{j+1} \to A_j$. Then $\lambda_{j+1} - \delta_*^i(\mu'_{j+1})$ is a map $P^i \to \ker(\phi_j)$ mapped to 0 by δ_*^i, and hence of the form $\delta_*^{i-1}(\nu_{j+1})$ with some $\nu_{j+1} : P_{i-1} \to \ker(\phi_j)$ by the assumption $H^i(G, \ker(\phi_j)) = 0$. Setting $\mu_{j+1} = \mu'_{j+1} + \nu_{j+1}$ completes the inductive step. □

We also need a lemma often called the additive form of Hilbert's theorem 90.

Lemma 6.10. *If $K|k$ is a finite Galois extension of fields with Galois group G, then $H^i(G, K) = 0$ for $i > 0$.*

Proof. The normal basis theorem of Galois theory asserts that there is an element $x \in K$ such that the images $\sigma(x)$ for $x \in G$ form a basis of K as a k-vector space. In other words, $K \cong k \otimes_{\mathbf{Z}} \mathbf{Z}[G]$ as a G-module and hence is *co-induced*. The claim follows.

Here is another argument which works for G cyclic and i even (and hence is sufficient to treat $H^2(G, K)$ for K finite which will be our most important application). Applying Lemma 4.10 to the G-module K we have to show that the map $\mathrm{Tr} := 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1} : K \to k$ is surjective, where n is the order of G and $\sigma \in G$ is a generator. By Dedekind's lemma the map Tr is not identically 0, so we find $x \in K$ with $\mathrm{Tr}(x) = a \in k^\times$. Now if $b \in k^\times$ is an arbitrary element, then

$$\mathrm{Tr}(a^{-1}bx) = \sum_{i=0}^{n-1} \sigma(a^{-1}bx) = \sum_{i=0}^{n-1} \sigma(a^{-1}b)\sigma(x) = a^{-1}b \sum_{i=0}^{n-1} \sigma(x) = a^{-1}b\mathrm{Tr}(x) = b.$$

□

Proof of Proposition 6.8. In view of Theorem 4.7 and the discussion preceding the proposition it will be enough to prove the first statement. Consider for all $j > 0$ the multiplicative subgroups

$$U_L^j := \{x \in L : \, v(x-1) \geq i\}$$

in the group of units U_L of L. The groups U_L^j form a decreasing filtration of U_L^1 such that the natural map $U_L^1 \to \varprojlim U_L^1/U_L^j$ is an isomorphism. Furthermore, the reduction map $U_L \to \lambda^\times$ yields an exact sequence

$$1 \to U_L^1 \to U_L \to \lambda^\times \to 1$$

whose associated long exact sequence shows that the proposition follows if we show $H^2(G, U_L^1) = 0$. For this, fix a local parameter π generating the maximal ideal of the valuation ring $A_v \subset L$ of v, and consider the maps $U_L^j \to \lambda$ sending $1 + a\pi^j$ to the image of $a \in A_v$ in λ. These maps are surjective group homomorphisms giving rise to exact sequences of G-modules

$$1 \to U_L^{j+1} \to U_L^j \to \lambda \to 0$$

for all j. Here we have $H^2(G, \lambda) = 0$ by Lemma 6.10, from which we infer $H^2(G, U_L^j/U_L^{j+1}) = 0$ for $j > 0$. By induction on j using the exact sequences

$$1 \to U_L^j/U_L^{j+1} \to U_L^1/U_L^{j+1} \to U_L^1/U_L^j \to 1$$

we obtain $H^2(G, U_L^1/U_L^j) = 0$ for all $j > 0$. We conclude by applying the above lemma to the inverse system of G-modules formed by the quotients U_L^1/U_L^j. □

Corollary 6.11 (Witt). *For a complete discretely valued field K with perfect residue field κ there is a split exact sequence*

$$0 \to \mathrm{Br}(\kappa) \to \mathrm{Br}(K) \to \mathrm{Hom}_c(\mathrm{Gal}(\bar{\kappa}|\kappa), \mathbf{Q}/\mathbf{Z}) \to 0. \tag{16}$$

Here $\bar{\kappa}$ is a fixed algebraic closure of κ and $\mathrm{Hom}_c(\mathrm{Gal}(\bar{\kappa}|\kappa), \mathbf{Q}/\mathbf{Z})$ denotes those homomorphisms $\mathrm{Gal}(\bar{\kappa}|\kappa) \to \mathbf{Q}/\mathbf{Z}$ that factor through a finite quotient of $\mathrm{Gal}(\bar{\kappa}|\kappa)$.

Proof. This follows from Corollary 6.1 and the above proposition after taking (directed) unions over L. □

Corollary 6.12 (Hasse). *Assume moreover κ is a finite field. Then $\mathrm{Br}(K) \cong \mathbf{Q}/\mathbf{Z}$.*

Proof. In this case $\mathrm{Br}(\kappa) = 0$ by Example 4.13 and $\mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z}) \cong \mathbf{Z}/n\mathbf{Z}$ if G has order n because a finite extension of finite fields has cyclic Galois group. □

Remark 6.13. The corollary applies in particular to the field $\mathbf{Q}_p$ of p-adic numbers and its finite extensions. It can be used to determine the Brauer group of $\mathbf{Q}$ via the following famous theorem of Albert, Brauer, Hasse, and Noether: there is an exact sequence

$$0 \to \mathrm{Br}(\mathbf{Q}) \to \bigoplus_p \mathrm{Br}(\mathbf{Q}_p) \oplus \mathrm{Br}(\mathbf{R}) \xrightarrow{\Sigma} \mathbf{Q}/\mathbf{Z} \to 0.$$

Here the maps $\mathrm{Br}(\mathbf{Q}) \to \mathrm{Br}(\mathbf{Q}_p)$ are induced by the base change maps $A \mapsto A \otimes_{\mathbf{Q}} \mathbf{Q}_p$ for a central simple $\mathbf{Q}$-algebra A; it is a nontrivial fact that for fixed A the algebras $A \otimes_{\mathbf{Q}} \mathbf{Q}_p$ are split for all but finitely many p. Similarly we have a map $\mathrm{Br}(\mathbf{Q}) \to \mathrm{Br}(\mathbf{R})$. The map Σ is induced by taking the isomorphisms $\mathrm{Br}(\mathbf{Q}_p) \cong \mathbf{Q}/\mathbf{Z}$, the embedding $\mathrm{Br}(\mathbf{R}) \to \mathbf{Q}/\mathbf{Z}$ induced by the inclusion $\frac{1}{2}\mathbf{Z}/\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}$ and then taking the sum. The theorem holds more generally for finite extensions of $\mathbf{Q}$; one then has to consider extensions of the p-adic and real valuations in the direct sum.