Brauer Group and Galois Cohomology

Jujian Zhang Yunzhou Xie

January 22, 2025

Contents

Preface

In this exposition, we describe a excruciatingly detailed proof of the following theorem:

Theorem. For a finite dimensional and Galois field extension K/F, the relative Brauer group $\mathrm{Br}(\mathsf{K}/\mathsf{F})$ is isomorphic to the second group cohomology $\mathrm{H}^2\left(\mathrm{Gal}(\mathsf{K}/\mathsf{F}), \mathsf{K}^\star\right)$.

The reason for the detailed-ness is because we are aiming to formalise the proof described in the following chapters; therefore the more details, the better. We apologise for the unconventional organisation in advance — earlier chapters sometimes use results from later chapter. For our defence, we try to categorise all the results by topics and, since this is a formalisation project, we can guarantee the readers that there is no circular reasoning.

Chapter 1

Central Simple Algebras

1.1 Basic Theory

In this chapter we define central simple algebras. We used some results in section 3.1.

Definition 1.1.1 (Simple Ring). A ring R is simple if the only two-sided-ideals of R are 0 and R. An algebra is simple if it is simple as a ring.

Remark 1.1.1. Division rings are simple.

Lemma 1.1.2. Let A be a simple ring, then centre of A is a field.

Proof. Let $0 \neq x$ be an element of centre of A. Then $I := \{xy | y \in A\}$ is a two-sided-ideal of A. Since $0 \neq x \in I$, we have that $I = A$. Therefore $1 \in I$, hence x is invertible. □

Definition 1.1.2 (Central Algebras). Let R be a ring and A an R-algebra, we say A is central if and only if the centre of A is R

Remark 1.1.3. Every commutative ring is a central algebra over itself.

Remark 1.1.4. Simpleness is invariant under ring isomorphism and centrality is invariant under algebra isomorphism.

Lemma 1.1.5. If A is a central R-algerba, A^{opp} is also central. .

Lemma 1.1.6. R is a simple ring if and only if any ring homomorphism $f : R \to S$ either injective or S is the trivial ring.

Proof. If R is simple, then the $\ker f$ is either $\{0\}$ or R. The former case implies that f is injective while the latter case implies that S is the trivial ring. Conversely, let $I \subseteq R$ be a two-sided-ideal. Consider $\pi : R \to {}^{R}/_{I}$, either π is injective implying that $I = \{0\}$ or that ${}^{R}/_{I}$ is the trivial ring implying that $I = R$. □

Remark 1.1.7. If A is a simple R-algebra, "ring homomorphism" in lemma 1.1.6 can be replaced with R-algebra homomorphism.

Corollary 1.1.8. Assume R is a field. Let A, B be finite dimensional R-algebras where A is simple as well. Then any R-algebra homomorphism $f : A \to B$ is bijective if $\dim_R A = \dim_R B$.

Proof. By lemma 1.1.6, fis injective. Then $\dim_K \operatorname{im} f = \dim_K B - \dim_K \ker f = \dim_K B$ meaning that f is surjective. □

Let K be a field and A, B be K-algebras.

Lemma 1.1.9. If A and B are central K-algebras, $A \otimes_K B$ is a central K-algebra as well.

Proof. Assume A and B are central algebras, then by corollary 3.1.7 $Z(A \otimes_R B) = Z(A) \otimes_R Z(B) = R \otimes_R R = R$. □

Theorem 1.1.10. If A is a simple K-algebra and B is a central simple K-algebra, $A \otimes_K B$ is a central simple K-algebra as well.

Proof. By lemma 1.1.9, we need to prove $A \otimes_K B$ is a simple ring. Denote f as the map $A \to A \otimes_K B$. It is sufficient to prove that for every two-sided-ideal $I \subseteq A \otimes_K B$, we have $I = \left\langle f\left(f^{-1}(I)\right)\right\rangle$. Indeed, since A is simple $f^{-1}(I)$ is either $\{0\}$ or A, if it is $\{0\}$, then $I = \{0\}$; if it is A, then I is A as well.

We will prove that $I \leqslant \left\langle f\left(f^{-1}(I)\right)\right\rangle$, the other direction is straightforward. Without loss of generality assume $I \neq \{0\}$. Let $\mathcal{A}$ be an arbitrary basis of A, by lemma 3.1.1, we see that every element $x \in A \otimes_K B$ can be written as $\sum_{i=0}^{n} \mathcal{A}_i \otimes b_i$ for some natrual number n and some choice of $b_i \in B$ and $\mathcal{A}_i \in \mathcal{A}$. Since I is not empty, we see there exists a non-zero element $\omega \in I$ such that its expansion $\sum_{i=0}^{n} \mathcal{A}_i \otimes b_i$ has the minimal n. In particular, all b_i are non-zero and $n \neq 0$. We have $\omega = \mathcal{A}_0 \otimes b_0 + \sum_{i=1}^{n} \mathcal{A}_i \otimes b_i$. Since B is simple, $1 \in B = \langle\langle b_0 \rangle\rangle$; hence we write $1 \in \sum_{j=0}^{m} x_i b_0 y_i$ for some $x_i, y_i \in B$. Define $\Omega := \sum_{j=0}^{m} (1 \otimes x_i)\omega(1 \otimes y_i)$ which is also in I. We write

$$\begin{aligned}
\Omega &= \mathcal{A}_0 \otimes \left(\sum_{j=0}^{m} x_j b_0 y_j\right) + \sum_{i=1}^{n} \mathcal{A}_i \otimes \left(\sum_{j=0}^{m} x_j b_i y_j\right) \\
&= \mathcal{A}_0 \otimes 1 + \sum_{i=1}^{n} \mathcal{A}_i \otimes \left(\sum_{j=0}^{m} x_j b_i y_j\right)
\end{aligned}$$

For every $\beta \in B$, we have that $(1 \otimes \beta)\Omega - \Omega(1 \otimes \beta)$ is in I and is equal to

$$\sum_{i=1}^{n} \mathcal{A}_i \otimes \left(\sum_{j=0}^{m} \beta x_j b_i y_j - x_j b_i y_j \beta\right),$$

which is an expansion of $n-1$ terms, thus $(1 \otimes \beta)\Omega - \Omega(1 \otimes \beta)$ must be 0. Hence we conclude that for all $i = 1, \ldots, n$, $\sum_{j=0}^{m} x_j b_i y_j \in Z(B) = K$. Hence for all $i = 1, \ldots, n$, we find a $\kappa_i \in K$ such that $\kappa_i = \sum_{j=0}^{m} x_j b_i y_j$. Hence we can calculate Ω as

$$\begin{aligned}
\Omega &= \mathcal{A}_0 \otimes 1 + \sum_{i=1}^{n} \mathcal{A}_i \otimes \left(\sum_{j=0}\right) \\
&= \mathcal{A}_0 \otimes 1 + \sum_{i=1}^{n} \mathcal{A}_i \otimes \kappa_i \qquad . \\
&= \left(\mathcal{A}_0 + \sum_{i=1}^{n} \kappa_i \cdot \mathcal{A}_i\right) \otimes 1
\end{aligned}$$

From this, we note that $\mathcal{A}_0 + \sum_i^n \kappa_i \cdot \mathcal{A}_i \in f^{-1}(I)$; since A is simple, we immediately conclude that $f^{-1}(I) = A$, once we know $\mathcal{A}_0 + \sum_{i=1}^n \kappa_i \cdot \mathcal{A}_i$ is not zero. If it is zero, by the fact that $\mathcal{A}$ is a linearly independent set, we conclude that $1, \kappa_1, \ldots, \kappa_n$ are all zero; which is a contradiction. Since $f^{-1}(I) = A$, we know $\langle f(f^{-1} I) \rangle = A \otimes_K B$. □

Corollary 1.1.11. Central simple algebras are stable under base change. That is, if L/K is a field extension and D is a central simple algebra over K, then $L \otimes_K D$ is central simple over L.

Proof. By theorem 1.1.10, $L \otimes_K D$ is simple. Let $x \in Z(L \otimes_K D)$, by corollary 3.1.7, we have $x \in Z(L) \otimes Z(D) = Z(L)$. Without loss of generality, we can assume that $x = l \otimes d$ is a pure tensor, then $l \in Z(L)$ and $d \in K$. Therefore $x = d \cdot l \in L$. □

Theorem 1.1.12. If $A \otimes_K B$ is a simple ring, then A and B are both simple.

Proof. By symmetry, we only prove that A is simple. If A or B is the trivial ring then $A \otimes_K B$ is the trivial ring, a contradiction. Thus we assume both A and B are non-trivial. Suppose A is not simple, by lemma 1.1.6, there exists a non-trivial K-algebra A' and a K-algebra homomorphism $f : A \to A'$ such that $\ker f \neq \{0\}$. Let $F : A \otimes_K B \to A' \otimes_K B$ be the base change of f, then since $A \otimes_K B$ is simple and $A' \otimes B$ is non-trivial (A' is non-trivial and B is faithfully flat because B is free), we conclude that F is injective. Then we have that

$$0 \xrightarrow{0} A \otimes_K B \xrightarrow{F} A' \otimes_K B$$

is exact. Since B is faithfully flat as a K-module, tensorig with B reflects exact sequences, therefore

$$0 \xrightarrow{0} A \xrightarrow{f} A'$$

is exact as well. This is contradiction since f is not injective. □

1.2 Subfields of Central Simple Algebras

Definition 1.2.1 (Subfield). For any field K and K-algebra A, a subfield $B \subseteq A$ is a commutative K-subalgebra of A that is closed under inverse for any non-zero member.

Remark 1.2.1. Subfields inherit a natural ordering from subalgebras.

Let K be any field and D a finite dimensional central division K-algebra and A a finite dimensional central simple algebra of A.

Lemma 1.2.2. Let k be a maximal subfield of D,

$$\dim_K D = (\dim_K k)^2.$$

Proof. By lemma 3.4.11, we have that $\dim_K D = \dim_K C_D(k) \cdot \dim_K k$. Hence it is sufficient to show that $C_D(k) = k$. By the commutativity of k, we have that $k \leqslant C_D(k)$. Suppose $k \neq C_D(k)$: let $a \in C_D(k)$ that is not in k. We see that $L := k(a)$ is another subalgebra of D that is strictly larger than k; a contradiction. Therefore $k = C_D(k)$ and the theorem is proved. □

Lemma 1.2.3. Suppose L is a subfield of A, the following are equivalent:

1. $L = C_A(L)$

2. $\dim_K A = (\dim_K L)^2$

3. for any commutative K-subalgebra $L' \subseteq A$, $L \subseteq L'$ implies $L = L'$

Proof. We prove the following:

- "1. implies 2.": this is lemma 3.4.11.
- "2. implies 1.": Since L is commutative, we always have $L \subseteq C_A(L)$. Hence we only need to show $\dim_K L = \dim_K C_A(L)$. This is because by lemma 3.4.11, we have that $\dim_K A = \dim_K L \cdot \dim_K C_A(L)$ and by 2. we have $\dim_K L \cdot \dim_K C_A(L) = \dim_K L \cdot \dim_K L$.
- "2. implies 3.": Since 2. implies 1., we assume $L = C_A(L)$, therefore all we need is to prove $L' \subseteq C_A(L)$. Let $x \in L'$ and $y \in L \subseteq L'$, we need to show $xy = yx$ which is commutativity of L'.
- "3. implies 1.": By commutativity of L, we always have $L \subseteq C_A(L)$. For the other direction, suppose $C_A(L) \nsubseteq L$, then there exists some $a \in C_A(L)$ but not in L. Consider $L' = L(a)$, by 3., we have $L' = L$ which is a contradiction.

□

Chapter 2

Morita Equivalence

This chapter intertwine with section 3.2: section 2.2 depends on section 3.2.1; while section 3.2.2 depends on section 2.2.

2.1 Construction of the equivalence

Let R be a ring and $0 \neq n \in \mathbb{N}$. In this chapter, we prove that the category R-modules and the category of $\mathrm{Mat}_n(R)$-modules are equivalent. Then we use the equivalence to prove several useful lemmas.

Construction 2.1.1. If M is an R-module, we have a natural $\mathrm{Mat}_n(R)$-module structure on $\widehat{M} := M^n$ given by $(m_{ij}) \cdot (v_k) = \sum_j m_{ij} \cdot v_j$. If $f : M \to N$ is an R-linear map, then $\widehat{f} : M^n \to N^n$ given by $(v_i) \mapsto (f(v_i))$ is a $\mathrm{Mat}_n(R)$-linear map. Thus we have a well-defined functor $\mathfrak{Mod}_R \Longrightarrow \mathfrak{Mod}_{\mathrm{Mat}_n(R)}$.

Remark 2.1.1. Note that all modules are assumed to be left modules; when we need to consider right R-modules, we will consider left R^{opp}-modules instead. We use δ_{ij} to denote the matrix whose (i, j)-th entry is 1 and 0 elsewhere. δ_{ij} forms a basis for matrices.

Construction 2.1.2. If M is a $\mathrm{Mat}_n(R)$-module, then $\widetilde{M} := \{\delta_{ij} \cdot m | m \in M\} \subseteq M$ is an R-module whose R-action is given by $r \cdot (\delta_{ij} \cdot m) := (r \cdot \delta_{ij}) \cdot m$. More over if $f : M \to N$ is a $\mathrm{Mat}_n(R)$-linear map, $\widetilde{f} : \widetilde{M} \to \widetilde{N}$ given by the restriction of f is R-linear. Hence, we have a functor $\mathfrak{Mod}_{\mathrm{Mat}_n(R)} \Longrightarrow \mathfrak{Mod}_R$.

Theorem 2.1.2 (Morita Equivalence). The functors constructed in construction 2.1.1 and construction 2.1.2 form an equivalence of category.

Proof. Let M be an R-module, then the unit $\widetilde{\widehat{M}} \cong M$ is given by

$$x \mapsto \sum_j x_j$$
$$(x, 0, \ldots, 0) \leftarrow x$$

Let M be an $\mathrm{Mat}_n(R)$-module, then the counit $\widehat{\widetilde{M}} \cong M$ is given by $m \mapsto (\delta_{i0} \cdot m)$. This map is both injective and surjective. □

2.2 Stacks 074E

Let A be a finite dimensional simple k-algebra.

Lemma 2.2.1. Let M and N be simple A-modules, then M and N are isomorphic as A-modules.

Proof. By theorem 3.2.6, there exists non-zero $n \in \mathbb{N}$, k-division algebra D such that $A \cong \mathrm{Mat}_n(D)$ as k-algebras. Then by theorem 2.1.2, we have equivalence of category $e : \mathfrak{Mod}_A \cong \mathfrak{Mod}_D$. Since simple module is a categorical notion (it can be defined in terms monomorphisms), $e(M)$ and $e(N)$ are simple D-modules. Since D is a division ring, $e(M)$ and $e(N)$ are isomorphic as D-modules, therefore M and N are isomorphic as A-modules. □

Lemma 2.2.2. Let M be an A-module, there exists a simple A-module S such that M is a direct sum of copies of S, i.e. $M \cong \bigoplus_{i\in\iota} S$ for some indexing set ι.

Proof. By theorem 3.2.6, there exists non-zero $n \in \mathbb{N}$, k-division algebra D such that $A \cong \mathrm{Mat}_n(D)$ as k-algebras. Then by theorem 2.1.2, we have equivalence of category $e : \mathfrak{Mod}_A \cong \mathfrak{Mod}_D$. Since simple module is a categorical notion (it can be defined in terms monomorphisms), $e^{-1}(D)$ is a simple module over A. Since $e(M)$ is a free module over D, we can write $e(M)$ as $\bigoplus_{i\in\iota} D$ for some indexing set ι. By precomposing the unit of e, we get an isomorphism $M \cong e^{-1}\left(\bigoplus_{i\in\iota} D\right)$. We only need to prove $e^{-1}\left(\bigoplus_{i\in\iota} D\right) \cong \bigoplus_{i\in\iota} e^{-1}(D)$. This is because direct sum is the categorical coproduct. □

Remark 2.2.3. Note that by lemma 2.2.1, any two simple A-module are isomorphic, hence for any A-module M and any simple A-module S, we can write M as a direct sum of copies of S.

Lemma 2.2.4. Let M and N be two finite A-module with compatible k-action. Then M and N are isomorphic as A-module if and only if $\dim_k M$ and $\dim_k N$ are equal.

Proof. The forward direction is trivial as an A-linear isomorphism is a k-linear isomorphism as well. Conversely, suppose $\dim_k M = \dim_k N$. By lemma 2.2.2, there exists a simple A-module S such that $M \cong \bigoplus_{i\in\iota} S$ and $N \cong \bigoplus_{i\in\iota'} S$ as A-modules. Without loss of generality $S \neq 0$, for otherwise we have $M \cong N$ anyway. If either of ι or ι' is empty, then $\dim_k M = \dim_k N = 0$ implying that $M = N = 0$, we again have $M \cong N$. Thus, we assume both ι and ι' are non-empty. By pulling back the A-module structure on S to a k-module structure along $k \hookrightarrow A$, $M, N, S, \bigoplus_{i\in\iota} S, \bigoplus_{i\in\iota'} S$ are all finite dimensional k-vector spaces. Hence ι and ι' are finite. The equality $\dim_k M = \dim_k N$ tells us that $\iota \cong \iota'$ as set, hence $M \cong \bigoplus_{i\in\iota} S \cong \bigoplus_{i\in\iota'} S \cong N$ as required. □

Let $A \cong \mathrm{Mat}_n(D)$ as k-algebras for some k-division algebra and $n \neq 0$.

Lemma 2.2.5. D^n is a simple A-module where the module structure is given by pulling back the $\mathrm{Mat}_n(D)$-module structure of D^n.

Proof. By theorem 2.1.2, we have $\mathfrak{Mod}_A \cong \mathfrak{Mod}_D \cong \mathfrak{Mod}_{\mathrm{Mat}_n(D)}$. Since D is a simple D-module, D^n is a simple $\mathrm{Mat}_n(D)$ module and consequently, a simple A-module. □

Remark 2.2.6. Note that any A-linear endomorphism of D^n is $\mathrm{Mat}_n(D)$-linear, and vice versa. Thus we have $\mathrm{End}_A(D^n) \cong \mathrm{End}_{\mathrm{Mat}_n(D)}(D^n)$ as k-algebras.

Lemma 2.2.7. $\mathrm{End}_A(D^n)$ is isomorphic to D^{opp} as k-algebras.

Proof. Indeed, we calculate:

$$\begin{aligned}
\operatorname{End}_A(D^n) &\cong \operatorname{End}_{\operatorname{Mat}_n(D)}(D^n) \\
&\cong \operatorname{End}_D D && \text{by theorem 2.1.2, } \mathfrak{Mod}_D \cong \mathfrak{Mod}_{\operatorname{Mat}_n D} \\
&\cong D^{opp}
\end{aligned}$$

□

Lemma 2.2.8. Let M be a simple A-module, then $\operatorname{End}_A M \cong D^{opp}$ as k-algebras.

Proof. By theorem 2.1.2, D^n is simple as A-module; hence by lemma 2.2.1, D^n and M are isomorphic as A-module. Lemma 2.2.7 gives the desired result. □

Remark 2.2.9. In particular, if M is a simple A-module, then $\operatorname{End}_A M$ is a simple k-algbera.

Lemma 2.2.10. Let M be a simple A-module, then $\operatorname{End}_A M$ has finite k-dimension.

Proof. By theorem 3.2.4, such D and n always exists. Hence we only need to show D^{opp} has finite k-dimension. Since $\dim_k A = \dim_k \operatorname{Mat}_n(D)$ are both finite, we conclude D^{opp} is finite as a k-vector space by pulling back the finiteness along $D \hookrightarrow \operatorname{Mat}_n(D)$. □

Remark 2.2.11. Note that for all A-module M, $\operatorname{End}_{\operatorname{End}_A M} M$ is a k-algebra as well, with $k \hookrightarrow \operatorname{End}_{\operatorname{End}_A M} M$ given by $a \mapsto (x \mapsto a \cdot x)$. Thus, we always have a k-algebra homomorphism $A \to \operatorname{End}_{\operatorname{End}_A M} M$ given by the A-action on M. When A is a simple ring, this map is injective.

Definition 2.2.1 (Balanced Module). For any ring A and A-module M, we say M is a balanced A-module, if the A-linear map $A \to \operatorname{End}_{\operatorname{End}_A M} M$ is surjective.

Remark 2.2.12. Balancedness is invariant under linear isomorphism.

Lemma 2.2.13. For any ring A, A is balanced as A-module.

Proof. If $f \in \operatorname{End}_{\operatorname{End}_A M} A$, then the image of $f(1)$ under $A \to \operatorname{End}_{\operatorname{End}_A} A$ is f again. □

We assume again that A is a finite dimensional simple k-algebra.

Lemma 2.2.14. Any simple A-module is balanced.

Proof. Indeed, if M is a simple A-module, then $A \cong \bigoplus_{i\in\iota} M$ for some indexing set ι by lemma 2.2.2. Since A is balanced, $\bigoplus_{i\in\iota} M$ is balanced. Let $g \in \operatorname{End}_{\operatorname{End}_A M} M$, we can define a corresponding $G \in \operatorname{End}_{\operatorname{End}_{\oplus_i M}}(\bigoplus_i M)$ by sending (v_i) to $(g(v_i))$. Since $\bigoplus_i M$ is balanced, we know that for some $a \in A$, G is the image of a under $A \to \operatorname{End}_{\operatorname{End}_{\oplus_i M}}(\bigoplus_i M)$. Then the image of a under $A \to \operatorname{End}_{\operatorname{End}_A M} M$ is g. □

Lemma 2.2.15. For any simple A-module M, we have $A \cong \operatorname{End}_{\operatorname{End}_A M} M$ as k-algebras.

Proof. The canonical map $A \to \operatorname{End}_{\operatorname{End}_A M} M$ is both injective and surjective, as M is a balanced A-module and A is a simple ring. □

Chapter 3

Results in Noncommutative Algebra

3.1 A Collection of Useful Lemmas

In section, we collect some lemmas that does not really belong to anywhere.

3.1.1 Tensor Product

Lemma 3.1.1. Let M and N be R-modules such that $\mathcal{C}_{i \in \iota}$ is a basis for N, then every elements of $x \in M \otimes_R N$ can be uniquely written as $\sum_{i \in \iota} m_i \otimes \mathcal{C}_i$ where only finitely many m_i's are non-zero

Proof. Given the basis $\mathcal{C}$, we have R-linear isomorphism $N \cong \bigoplus_{i \in \iota} R$, hence $M \otimes_R N \cong \bigoplus_{i \in \iota} (M \otimes_R R) \cong \bigoplus_{i \in \iota} M$ as R-modules. □

By switching M and N, the symmetric statement goes without saying.

Lemma 3.1.2. Let K be a field, M and N be flat K-modules. Suppose $p \subseteq M$ and $q \subseteq N$ are K-submodules, then $(p \otimes_K N) \sqcap (M \otimes_K q) = p \otimes_K q$ as K-submodules.

Proof. The hard direction is to show $(p \otimes_R N) \sqcap (M \otimes_R q) \leqslant p \otimes_R q$. Consider the following diagram:

$$\begin{array}{ccccc} p \otimes_K q & \xrightarrow{u} & M \otimes_K q & \xrightarrow{v} & {}^{M}/_{p} \otimes_K q \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ p \otimes_K N & \xrightarrow{u'} & M \otimes_K N & \xrightarrow{v'} & {}^{M}/_{p} \otimes_K N \end{array}$$

Since ${}^{M}/_{p}$ is flat, γ is injective. Let $z \in (p \otimes_R N) \sqcap (M \otimes_R q) = \operatorname{im} \beta \sqcap \operatorname{im} u'$. By abusing notation, replace z with some elements of $M \otimes_K q$ and continue with $\beta(z) \in \operatorname{im} \beta \sqcap \operatorname{im} u'$. Since $v'(\beta(z)) = \gamma(v(z))$ and that $\beta(z) \in \operatorname{im} u'$, we conclude that $\gamma(v(z)) = 0$, that is $z \in \ker v = \operatorname{im} u$. We abuse notation again, let $z \in p \otimes_K q$, we need to show $\beta(u(z)) \in \operatorname{im} \beta \sqcap \operatorname{im} u'$, but $\beta \circ u = u' \circ \alpha$, we finish the proof. □

3.1.2 Centralizer and Center

Let R be a commutative ring and A, B be two R-algebras. We denote centralizer of $S \subseteq A$ by $C_A S$ and centre of A by $Z(A)$.

Lemma 3.1.3. Let S, T be two subalgebras of A, then $C_A(S \sqcup T) = C_A(S) \sqcap C_A(T)$.

This lemma can be generalized to centralizers of arbitrary supremum of subalgebras.

Lemma 3.1.4. If we assume B is free as R-module, then for any R-subalgebra S, we have that $C_{A \otimes_R B}(\mathrm{im}(S \to A \otimes_R B))$ is $C_A(S) \otimes_R B$

A symmetric statement goes without saying.

Proof. Let $w \in C_{A \otimes_R B}(\mathrm{im}(S \to A \otimes_R B))$. Since B is free, we choose an arbitrary basis $\mathcal{B}$; by lemma 3.1.1, we write $w = \sum_i m_i \otimes_K \mathcal{B}_i$. It is sufficient to show that $m_i \in C_A(S)$ for all i. Let $a \in S$, we need to show that $m_i \cdot a = a \cdot m_i$. Since w is in the centralizer, $w \cdot (a \otimes 1) = (a \otimes 1) \cdot w$. Hence we have $\sum_i (a \cdot m_i) \otimes \mathcal{B}_i = \sum_i (m_i \cdot a) \otimes \mathcal{B}_i$. By the uniqueness of lemma 3.1.1, we conclude $a \cdot m_i = m_i \cdot a$. □

Remark 3.1.5. A useful special case is when $S = A$, then since $C_A(A) = Z(A)$, we have $C_{A \otimes_R B}(\mathrm{im}(A \to A \otimes_R B))$ is equal to $Z(A) \otimes_R B$. Since $\mathrm{im}(R \otimes_R B \to A \otimes_R B) = \mathrm{im}(A \to A \otimes_R B)$, we conclude its centralizer in $A \otimes_R B$ is $Z(A) \otimes_R B$.

Corollary 3.1.6. Assume R is a field. Let S and T be R-subalgebras of A and B respectively. Then $C_{A \otimes_R B}(S \otimes_R T)$ is equal to $C_A(S) \otimes_R C_B(T)$

Proof. From lemma 3.1.2, $C_A(S) \otimes_R C_B(T)$ is equal to $(C_A(S) \otimes_R B) \sqcap (A \otimes_R C_B(T))$. The left hand side $C_A(S) \otimes_R B$ is equal to $C_{A \otimes_R B}(\mathrm{im}(S \to A \otimes_R B))$ and the right hand side is equal to $C_{A \otimes_R B}(\mathrm{im}(T \to A \otimes_R B))$. Hence by lemma 3.1.3, their intersection is equal to

$$C_{A \otimes_R B}(\mathrm{im}(S \to A \otimes_R B) \sqcup \mathrm{im}(T \to A \otimes_R B))$$

This is precisely $C_{A \otimes_R B}(S \otimes_R T)$. □

Corollary 3.1.7. Assume R is a field. The centre of $A \otimes_R B$ is $Z(A) \otimes_R Z(B)$.

Proof. Special case of corollary 3.1.6. □

3.1.3 Some Isomorphisms

Construction 3.1.1. Let R be a commutative ring and A an R-algebra. Then we have an R-algebra homomorphism $A \otimes_R A^{\mathrm{opp}} \cong \mathrm{End}_R A$ given by $a \otimes 1 \mapsto (a \cdot \bullet)$ and $1 \otimes a \mapsto (\bullet \cdot a)$. When R is a field and A is a finite dimensional central simple algebra, this morphism is an isomorphism by corollary 1.1.8.

Construction 3.1.2. Let A be an R-algebra and M an A-module. We have isomorphism $\mathrm{End}_A(M^n) \cong \mathrm{Mat}_n(\mathrm{End}_A M)$ as R-algebras. For any $f \in \mathrm{End}_A(M^n)$, we define a matrix M whose (i,j)-th entry is

$$x \mapsto f(0, \ldots, x, \ldots, 0)_i,$$

where x is at the j-th position. On the other hand, if $M \in \mathrm{Mat}_n(\mathrm{End}_A M)$, we define an A-linear map $f : M^n \to M^n$ by

$$v \mapsto \left(\sum_j M_{ij} v_j\right)_i .$$

Construction 3.1.3. Let A be an R-algebra. Then $\mathrm{Mat}_m(\mathrm{Mat}_n(A)) \cong \mathrm{Mat}_{mn}(A)$. The trick is to think $\mathrm{Mat}_m A$ as $\{0, \ldots, m-1\} \times \{0, \ldots, m-1\} \to A$. Since the indexing set $\{0, \ldots, mn-1\}$ bijects with $(\{0, \ldots, m-1\} \times \{0, \ldots, n-1\})$, the isomorphism is just function currying, function uncurrying, precomposing and postcomposing bijections.

Construction 3.1.4. Let A, B be R-algebras. Then $\mathrm{Mat}_{mn}(A \otimes_R B) \cong \mathrm{Mat}_m(A) \otimes_R \mathrm{Mat}_n B$ as K-algebras. We first construct R-algebra isomorphism $A \otimes_R \mathrm{Mat}_n(R) \cong \mathrm{Mat}_n(A)$:

$$\begin{aligned} &a \otimes 1 \mapsto \operatorname{diag} a \text{ and } 1 \otimes (m_{ij}) \mapsto (m_{ij}) \\ &\sum_{i,j} m_{ij} \otimes \delta_{ij} \leftarrow\!\shortmid (m_{ij}), \end{aligned}$$

where diag is the diagonal matrix and δ_{ij} the matrix whose only non-zero entry is at (i,j)-th and is equal to 1. Thus $\mathrm{Mat}_m(A) \otimes_R \mathrm{Mat}_n(B) \cong (A \otimes_R B) \otimes_R (\mathrm{Mat}_m(R) \otimes_R \mathrm{Mat}_n(R))$ as R-algebra. The Kronecker product gives us an R-algebra map $\mathrm{Mat}_m(R) \otimes_R \mathrm{Mat}_n(R) \to \mathrm{Mat}_{mn}(R)$. We want this map to be an isomorphism. By lemma 1.1.6, we only need to prove it to be surjective: for all $\delta_{ij} \in \mathrm{Mat}_{mn}(R)$, we interpret $\mathrm{Mat}_{mn}(R)$ as a function $\{0, \ldots, m-1\} \times \{0, \ldots, n-1\} \to R$, then δ_{ij} is the image of $\delta_{ab} \otimes \delta_{cd} \in \mathrm{Mat}_m(R) \otimes_R \mathrm{Mat}_n(R)$ where $i = (a, c)$ and $j = (b, d)$. Combine everything together, we see $\mathrm{Mat}_{mn}(A \otimes_R B)$ is isomorphic to $\mathrm{Mat}_{mn}(A \otimes_R B)$ as R-algebras.

3.2 Wedderburn-Artin Theorem for Simple Rings

3.2.1 Classification of Simple Rings

Lemma 3.2.1 (minimal ideal of simple rings). Let A be a ring and I a non-trivial minimal left ideal of A, then I is a simple A-module.

Proof. Let $J \leqslant I$ be an A-submodule of I, suppose J is non-trivial, we prove that $J = I$. Then the image J' of J under $I \hookrightarrow A$ is a non-trivial left ideal of A. Since $I \hookrightarrow A$ is injective, it is sufficient to prove that $J' = I$. This is because $J' \leqslant I$ and $J' \not< J$. □

Lemma 3.2.2. Let A be a simple ring and I a non-trivial left ideal. One can write $1 \in A$ as $\sum_{i=0}^n x_i y_i$ for some $x_i \in I$ and $y_i \in A$.

Proof. Let I' be the two-sided ideal spanned by I. Then since A is a simple ring, $I' = A$. Thus $1 \in I'$. One can write $1 \in A$ as $\sum_i a_i x_i b_i$ for some $x_i \in I$ and $a_i, b_i \in A$, since I is a left ideal $a_i x_i \in I$ as well. □

Now, we can find the smallest n such that $1 \in A$ can be written as $\sum_{i=0}^n x_i y_i$ for some $x_i \in I$ and $y_i \in A$. Let us fix the notations n, x_i and y_i

Lemma 3.2.3. The n, x_i and y_i are all non-zero.

Proof. If n is 0, then $1 = 0$ in A, but all simple rings are non-trivial. We argue by contradiction to prove that all x_i and y_i are non-zero. Assume there exists a j such that $y_j \neq 0$ implies $x_j = 0$. Without loss of generality, we assume $j = 0$. Then $1 = \sum_{i=0}^{n} x_i y_i = \sum_{i=1}^{n} x_i y_i$. This contradicts the minimality of n. □

Theorem 3.2.4 (Wedderburn). *Let A be a simple ring and I a non-trivial minimal left ideal. Then there exists a non-zero $n \in \mathbb{N}$ such that $A \cong I^n$ as A-modules.*

Proof. We continue to write $1 = \sum_{i=0}^{n} x_i y_i$ in the shortest possible manner. Then we can define an A-linear map $g : I^n \to A$ by $(v_i) \mapsto \sum v_i y_i$. Then g is surjective: if $a \in A$, then $(a x_i)$ is mapped to a under g. g is injective as well: support $g(v_i) = 0 = \sum_i v_i y_i$ with (v_i) not all zero. Without loss of generality, we assume $v_0 \neq 0$, then the ideal $\langle v_0 \rangle$ is equal to I (since I is simplelemma 3.2.1). Thus $x_0 \in I = \langle v_0 \rangle$; implying that $x_0 = r \cdot v_0$ for some $r \in A$. Thus $1 = 1 - r \cdot 0 = \sum_{i=0}^{n} x_i y_i - \sum_{i=0}^{n} r \cdot v_i y_i$. In this way, we cancelled the term at $i = 0$, contradicting the minimality of n. Hence g is an isomorphism. □

Theorem 3.2.5 (Wedderburn-Artin (Ideal)). *Let A be an Artinian simple ring. There exists a non-zero n and an ideal $I \subseteq A$ such that I is simple as an A-module and $A \cong I^n$ as A-module.*

Proof. By theorem 3.2.4, we only need a minimal left ideal. Since A is Artinian, such ideal exists. □

Theorem 3.2.6 (Wedderburn-Artin (Algebra)). *Let K be a field and B an finite dimensional simple algebra over K. There exists a non-zero $n \in \mathbb{N}$ and a division K-algebra S such that $B \cong \mathrm{Mat}_n(S)$.*

Proof. By theorem 3.2.5, we can find a n and a minimal left ideal I such $A \cong I^n$ as A-modules. Note that $(\mathrm{End}_B\, I)^{\mathrm{opp}}$ is a division ring. Then since $B^{\mathrm{opp}} \cong \mathrm{End}_B\, B \cong \mathrm{End}_B(I^n) \cong \mathrm{Mat}_n\,(\mathrm{End}_B\, I)$ as rings where the final isomorphism is from construction 3.1.2, we have $e : B \cong \mathrm{Mat}_n\,(\mathrm{End}_B\, I)^{\mathrm{opp}}$ as rings. We also have a K-algebra structure on $(\mathrm{End}_B\, I)^{\mathrm{opp}}$ given by $(a \cdot f)(x) = f(a \cdot x)$, and this algebra structure promotes the ring isomorphism e to a k-algebra isomorphism. □

3.2.2 Uniqueness of the Classification

In the previous section, we know that finite dimensional simple K-algebra B over is in fact a matrix algebras of a division K-algebra S. In this section, we prove that the division algebra S is essentially unique.

Theorem 3.2.7 (Uniqueness of Wedderburn-Artin theorem). *Let B be a finite-dimensional simple K-algebra. Suppose B is isomorphic as k-algebras to both $\mathrm{Mat}_n(D)$ and $\mathrm{Mat}_{n'}(D')$ where n, n' are non-zero natural numbers and D, D' are k-division algebra, then $n = n'$ and $D \cong D'$ as k-algebras.*

Proof. Since D^n is a simple B-module, by lemma 2.2.8, we see that $\mathrm{End}_A\, D^n \cong D^{\mathrm{opp}}$ and $\mathrm{End}_A\, D^n \cong D'^{\mathrm{opp}}$ as k-algebras. Thus $D^{\mathrm{opp}} \cong D'^{\mathrm{opp}}$ as k-algebras, consequently $D \cong D'$ as k-algebras as well. Since $A \cong \mathrm{Mat}_n(D) \cong \mathrm{Mat}_{n'}(D') \cong \mathrm{Mat}_{n'}(D)$ as k-algebras and A is finite k-dimensional, a dimension argument shows that $n = n'$. □

3.3 Skolem-Noether Theorem

Let K be a field, A, B be K-algebras where A is central simple and finite K-dimensional and B is simple. Let M be a simple A-module.

Construction 3.3.1. For any K-algebra homomorphism $f : B \to A$, we give M a $B \otimes_K \mathrm{End}_A M$-module structure by defining $(b \otimes l) \cdot m$ to be $f(b) \cdot l(m)$. To emphasis f, we denote M with the $B \otimes_K \mathrm{End}_A M$-module structure by M^f.

Lemma 3.3.1. Let $f : B \to A$ be a K-algebra homomorphism, M^f is finitely generated as a $B \otimes_K \mathrm{End}_A M$-module.

Proof. Since M is a finite A-module and A a finite dimensional K-vector space, M is a finite dimensional K-vector space as well. Suppose $S \subseteq M$ generates M as K-module, the claim is that S generates M^f as well. Let $x \in M^f$, we write $x = \sum_i \lambda_i \cdot s_i$ with $\lambda_i \in K$ and $s_i \in S$. Note that $\lambda_i \cdot s_i = (\rho(\lambda_i) \otimes 1_M)$ in M^f where $\rho : K \to B$ is the map giving B its K-algebra structure. Hence x is in the span of S in M^f as well. □

Remark 3.3.2. Given that B is simple, any k-algebra homomorphism $f : B \to A$ injective; therefore by finite K-dimensionality of A, B is finite K-dimensional as well.

Lemma 3.3.3. Let $f, g : B \to A$ be two K-algebra homomorphisms. Then M^f and M^g are isomorphic as $B \otimes_K \mathrm{End}_A M$-module.

Proof. By lemma 2.2.4, it is sufficient to prove $\dim_K M^f = \dim_K M^g$. But as K-vector space, M^f and M^g are literally M. □

Theorem 3.3.4 (Skolem-Noether). Let $f, g : B \to A$ be two K-algebra homomorphism. Then f and g differ only by a conjugation. That is there exists a unit $x \in A^\times$ such that $g = xfx^{-1}$.

Proof. Let M be any simple A-module (which exists by lemma 2.2.5). By lemma 3.3.3, we have some isomorphism $\phi : M^f \cong M^g$ as $B \otimes_K \mathrm{End}_A M$-module. Since M is simple, we have that M is a balanced A-module by lemma 2.2.15. Let e denote the k-algerba isomorphism $A \cong \mathrm{End}_{\mathrm{End}_A M} M$ given by the A-action on M. Since both ϕ and ϕ^{-1} defines an element of $\mathrm{End}_{\mathrm{End}_A M} M$, we define $a := e^{-1}(\phi)$ and $b := e^{-1}(\phi^{-1})$. Then $ab = 1$ since $e(ab) = e(a) \cdot e(b) = \phi\phi^{-1} = 1$. We prove that the image of f and afb under e are the same; that is for all $x \in B$ and $m \in M$, $e(g(x))(m) = e(af(x)b)(m)$. The right hand side is equal to

$$\begin{aligned} e(af(x)b)(m) &= (e(a) \circ e(f(x)) \circ e(b))\,(m) \\ &= \left(\phi \circ e(f(x)) \circ \phi^{-1}\right)(m) \quad . \\ &= \phi\left(f(x) \cdot \phi^{-1}(m)\right) \end{aligned}$$

Similarly, the left hand side is equal to $g(x) \cdot m$. Note that ϕ is $B \otimes \mathrm{End}_A M$-linear. Therefore $\phi\left((x \otimes 1) \cdot \phi^{-1}(m)\right) = (x \otimes 1) \cdot m$. Unfolding the definition of M^f and M^g, we see this is saying precisely $\phi\left(f(x) \cdot \phi^{-1}(m)\right) = g(x) \cdot m$. □

3.4 Double Centralizer Theorem

In this section let F be a field and A an F-algebra. Define $\mathcal{L}_A \subseteq \operatorname{End}_F A$ to be

$$\{f : A \to A | f(x) = ax \text{ for some } a \in A\},$$

i.e. F-linear maps defined by left multiplication; similarly define $\mathcal{R}_A$. Note that $\mathcal{L}_A$ and $\mathcal{R}_A$ are F-subalgebras of $\operatorname{End}_F A$. When we need to stree the underlying field is F, we also write $\mathcal{L}_A^F$ and $\mathcal{R}_A^F$. We assume A to be a finite dimensional central simple F-algebra.

Lemma 3.4.1. The centralizer of $\mathcal{L}_A$ in $\operatorname{End}_F A$ is smaller than or equal to $\mathcal{R}_A$:

$$C_{\operatorname{End}_F A}(\mathcal{L}_A) \leqslant \mathcal{R}_A.$$

Proof. Indeed, let $x \in C_{\operatorname{End}_F A}(\mathcal{L}_A)$. Recall from construction 3.1.1 that $e : A \otimes_F A^{\mathsf{opp}} \cong \operatorname{End}_F A$ as F-algebras. Then $e^{-1}(x)$ is in $C_{A \otimes_F A^{\mathsf{opp}}}(\operatorname{im}(A \to A \otimes_F A^{\mathsf{opp}}))$ (for e sends $a \otimes 1$ to the F-linear map $(a \cdot \bullet)$). Since $C_{A \otimes_F A^{\mathsf{opp}}}(\operatorname{im}(A \to A \otimes_F A^{\mathsf{opp}})) = Z(A) \otimes_F A^{\mathsf{opp}} = F \otimes_F A^{\mathsf{opp}} = \operatorname{im}(A^{\mathsf{opp}} \to A \otimes_F A^{\mathsf{opp}})$, we find some $y \in A^{\mathsf{opp}}$ such that $1 \otimes y = e^{-1}(x)$. Therefore $e(1 \otimes y) = x$; but $e(1 \otimes y)$ is in $\mathcal{R}_A$ for it is the linear map $(\bullet \cdot y)$. □

Remark 3.4.2. For any F-algebra B, every element in $C_{\operatorname{End}_F B}(\mathcal{L}_B)$ is in fact $Z(B)$-linear. Let $x \in C_{\operatorname{End}_F B}(\mathcal{L}_B)$, $z \in Z(B)$ and $b \in B$, we have $x(z \cdot b) = z \cdot x(b)$ because x commutes with the linear map $(z \cdot \bullet)$.

Remark 3.4.3. A is a $Z(A)$-algebra whose algebra structure is given by $Z(A) \hookrightarrow A$. By lemma 1.1.2, $Z(A)$ is a field. A is finite dimensional as a $Z(A)$-module because of the tower $A/Z(A)/F$.

Lemma 3.4.4. As F-algebras, we have $\mathcal{R}_A \cong A^{\mathsf{opp}}$.

Proof. We prove the map $A^{\mathsf{opp}} \to \mathcal{R}_A$ is bijective. It is injective because if $(\bullet \cdot a) = (\bullet \cdot b)$, then $a = 1 \cdot a = 1 \cdot b = b$. The map is surjective by the definition of $\mathcal{R}_A$. □

Lemma 3.4.5. Let B be any simple F-algebra (not necessarily central). The centralizer of $\mathcal{L}_B$ in $\operatorname{End}_F B$ is equal to $\mathcal{R}_B$.

Proof. It is straightforward to show $\mathcal{R}_B^F \leqslant C_{\operatorname{End}_F A}(\mathcal{L}_B^F)$. So we only need to prove $C_{\operatorname{End}_F A}(\mathcal{L}_B^F) \leqslant \mathcal{R}_B^F$. By lemma 3.4.1, since B is a central simple finite dimensional $Z(B)$-algebra, we have that

$$C_{\operatorname{End}_{Z(B)} B}\left(\mathcal{L}_B^{Z(B)}\right) \leqslant \mathcal{R}_B^{Z(B)}.$$

Suppose $f \in \operatorname{End}_F B$ is in $C_{\operatorname{End}_F B} B$, by remark 3.4.2, f is $Z(B)$-linear as well. Then f is in $\mathcal{R}_B^{Z(B)}$; that is f is equal to $(\bullet \cdot b)$ for some $b \in B$ as $Z(B)$-linear maps. Then f is also equal to $(\bullet \cdot b)$ as F-linear maps. □

Construction 3.4.1. Let B be any F-algebra and $S \subseteq B$ an F-subalgebra. For any $x \in B^\times$, we have that $xSx^{-1} := \{xsx^{-1} | s \in S\}$ is an F-subalgebra of B as well. We have the obvious F-algebra isomorphism $S \cong xSx^{-1}$ given by $s \mapsto xsx^{-1}$ and $x^{-1}tx \mapsfrom t$. Therefore $\dim_F S = \dim_F xSx^{-1}$ and S is a simple ring if and only if xSx^{-1} is a simple ring.

Lemma 3.4.6. Let B be any F-algebra, $x \in B^\times$ and $S \subseteq B$ be an F-subalgebra of B, then $C_B(xSx^{-1}) = x(C_B(S))x^{-1}$.

Proof. If $a \in C_B\left(xSx^{-1}\right)$, then $x^{-1}ax$ is in $C_B(S)$. Conversely if a is equal to xbx^{-1} with $b \in C_B(S)$, then it is in $C_B\left(xSx^{-1}\right)$ as well. $\square$

Remark 3.4.7. For any finite dimensional F-module B, we have isomorphism $\operatorname{End}_F B \cong \operatorname{Mat}_{\dim_F B} F$ as F-algebras. Hence $\operatorname{End}_F B$ is a finite-dimensional central simple algebra over F.

Lemma 3.4.8. *Let $S \subseteq A$ be a simple F-subalgebra, then $A \otimes_F \mathcal{R}_S$ is a simple ring.*

Proof. By lemma 3.4.4, we have $A \otimes \mathcal{R}_S \cong A \otimes S^{opp}$ as F-algebras. The claim follows from theorem 1.1.10. $\square$

Lemma 3.4.9. *Let $S \subseteq A$ be a simple F-subalgebra, then there exists an $x \in (A \otimes_F \operatorname{End}_F S)^\times$ such that $C_A(S) \otimes_F \operatorname{End}_F S$ is isomorphic to $x\,(A \otimes_F \mathcal{R}_S)\,x^{-1}$ as F-algebras.*

Proof. By lemma 1.1.9 and theorem 1.1.10, $A \otimes_F C_A(S)$ is a central simple F-algebra. Let $f : S \to A \otimes_F \operatorname{End}_F S$ be an F-algebra homomorphism defined by $s \mapsto s \otimes 1_S$ and $g : S \to A \otimes_F \operatorname{End}_F S$ be an F-algebra homomorphism defined by $1_A \otimes (s \cdot \bullet)$. Then by theorem 3.3.4, we that there exists some $x \in (A \otimes_F \operatorname{End}_F S)^\times$ such that $f = xgx^{-1}$. Then we have $S \otimes_F \operatorname{End}_F S$ is equal to $x\,(A \otimes_F \mathcal{L}_S)\,x^{-1}$: indeed the left hand side is $\operatorname{im} f$ while the right handside is $x\,(\operatorname{im} g)\,x^{-1}$. Therefore $C_{A\otimes_F \operatorname{End}_F S}\,(S \otimes_F \operatorname{End}_F S) = C_{A\otimes_F \operatorname{End}_F S}\left(x\,(A \otimes_F \mathcal{R}_S)\,x^{-1}\right)$. By lemma 3.4.6, the right hand side is equal to $xC_{A\otimes_F \operatorname{End}_F S}\,(A \otimes_F \mathcal{L}_S)\,x^{-1}$ which is $x\,(A \otimes_F C_{\operatorname{End}_F S}\,(\mathcal{L}_S))\,x^{-1}$ by lemma 3.1.4 which is $x\,(A \otimes_F \mathcal{R}_S)\,x^{-1}$ by lemma 3.4.5. $\square$

Lemma 3.4.10. *Let $S \subseteq A$ be a simple F-subalgebra, then $C_A(S)$ is simple as well.*

Proof. By lemma 3.4.9, $C_A(S) \otimes_F \operatorname{End}_F S$ is isomorphic to $x\,(A \otimes_F \mathcal{R}_S)\,x^{-1}$ as F-algebras. Then $C(S) \otimes_F \operatorname{End}_F S$ is simple since $A \otimes_F \mathcal{R}_S$ is simple by lemma 3.4.8. By theorem 1.1.12, $C_A(S)$ is simple. $\square$

Lemma 3.4.11. *Let $S \subseteq A$ be a simple F-subalgebra. Then*

$$\dim_F C_A(S) \cdot \dim_F S = \dim_F A.$$

Proof. By lemma 3.4.9, $C_A(S) \otimes_F \operatorname{End}_F S$ is isomorphic to $x\,(A \otimes_F \mathcal{R}_S)\,x^{-1}$ as F-algebras. Hence $\dim_F\,(C_A(S) \otimes_F \operatorname{End}_F S) = \dim_F\,(A \otimes_F \mathcal{R}_S)$ where the left hand side is $\dim_F C_A(S) \cdot \dim_F \operatorname{End}_F S$ and the right hand side is $\dim_F A \cdot \dim_F \mathcal{R}_S$. Since $\dim_F \operatorname{End}_F S = \dim_F S^2$ and $\dim_F \mathcal{R}_S = \dim S$ (by lemma 3.4.4), we proved this lemma. $\square$

Corollary 3.4.12. *Let $S \subseteq A$ be a central simple F-subalgebra,*

$$A \cong B \otimes_F C_A(B).$$

Proof. By lemma 3.4.10, $C_A(B)$ is simple and by theorem 1.1.10, $B \otimes_F C_A(B)$ is simple. Hence the map $B \otimes_F C_A(B) \to A$ induced by $B \hookrightarrow A$ and $C_A(B) \hookrightarrow A$ is injective. By corollary 1.1.8, we only need to show $\dim_F B \otimes_F C_A(B) = \dim_F A$ which is precisely lemma 3.4.11. $\square$

Theorem 3.4.13 (Double Centralizer)**.** *Let $S \subseteq A$ be a simple F-subalgebra, we have*

$$C_A\,(C_A(S)) = S.$$

Proof. It is straightforward that $S \leqslant C_A\,(C_A(S))$. By lemma 3.4.10, $C_A(S)$ is simple, hence $\dim_F C_A\,(C_A(S)) \cdot \dim_F C_A(S) = \dim_F A = \dim_F C_A(S) \cdot \dim_F S$ (by applying lemma 3.4.11 twice), i.e. $\dim_F C_A\,(C_A(S)) = \dim_F S$. This equality of dimension gives us the desired result. $\square$

Chapter 4

Brauer Group

4.1 Construction of Brauer Group

Let K be a field. We denote the class of finite dimensional central simple K-algebras as CSA_K. When K is clear, we drop the subscript.

Remark 4.1.1. By lemma 1.1.9 and theorem 1.1.10, CSA is closed under tensor product, that is if $A, B \in \mathsf{CSA}$, we have $A \otimes_K B \in \mathsf{CSA}$ as well.

Definition 4.1.1 (Brauer Equivalence). For any two $A, B \in \mathsf{CSA}$, we say A and B are Brauer equivalent, when there exists $m, n \in \mathbb{N}_{\geqslant 0}$ such that $\mathrm{Mat}_m(A) \cong \mathrm{Mat}_n B$ as K-algebras. We denote this relation as $A \sim_{\mathrm{Br}_K} B$, when K is clear, we drop the subscript.

Remark 4.1.2. Isomorphic K-algebras are Brauer equivalent.

Lemma 4.1.3. $\sim_{\mathrm{Br}}$ is reflexive.

Proof. Indeed, $A \cong \mathrm{Mat}_1(A)$ as K-algerbas. □

Lemma 4.1.4. $\sim_{\mathrm{Br}}$ is symmetric.

Proof. Indeed, just exchange m and n. □

Lemma 4.1.5. $\sim_{\mathrm{Br}}$ is transitive.

Proof. Let $A \sim_{\mathrm{Br}} B$ and $B \sim_{\mathrm{Br}} C$; that is for some $m, n, p, q \in \mathbb{N}_{\geqslant 0}$ we have $\mathrm{Mat}_n(A) \cong \mathrm{Mat}_m(B)$ and $\mathrm{Mat}_p(B) \cong \mathrm{Mat}_q(C)$ as K-algebras. Hence, from construction 3.1.3, we have the following:

$$\begin{aligned}
\mathrm{Mat}_{np}(A) &\cong \mathrm{Mat}_p\left(\mathrm{Mat}_n(A)\right) \cong \mathrm{Mat}_p\left(\mathrm{Mat}_m(B)\right) \\
&\cong \mathrm{Mat}_{mp}(B) \cong \mathrm{Mat}_m\left(\mathrm{Mat}_p(B)\right) \\
&\cong \mathrm{Mat}_m\left(\mathrm{Mat}_q(C)\right) \cong \mathrm{Mat}_{mq}(C).
\end{aligned}$$

In another word, $A \sim_{\mathrm{Br}} C$. □

Hence $\sim_{\mathrm{Br}}$ is really an equivalence relation, we denote the quotient ${}^{\mathsf{CSA}}/_{\sim_{\mathrm{Br}}}$ as $\mathrm{Br}(K)$.

Lemma 4.1.6. $(\bullet \otimes_K \bullet) : \mathsf{CSA} \times \mathsf{CSA} \to \mathsf{CSA}$ descends to a function on $\mathrm{Br}(K)$.

Proof. We need to prove that for all $A, B, C, D \in \mathsf{CSA}$ such that $A \sim_{\mathrm{Br}} B$ and $C \sim_{\mathrm{Br}} D$, $A \otimes_R C \sim_{\mathrm{Br}} B \otimes_R D$ as well. Suppose $\mathrm{Mat}_m(A) \cong \mathrm{Mat}_n(B)$ as K-algebras and $\mathrm{Mat}_p(C) \cong \mathrm{Mat}_q(D)$, by construction 3.1.4, we have

$$\begin{aligned}\mathrm{Mat}_{mp}(A \otimes_R C) &\cong \mathrm{Mat}_m(A) \otimes_R \mathrm{Mat}_p(C)\\ &\cong \mathrm{Mat}_n(B) \otimes_R \mathrm{Mat}_q(D)\\ &\cong \mathrm{Mat}_{nq}(B \otimes_R D).\end{aligned}$$

□

Construction 4.1.2 (Brauer Group). $\mathrm{Br}(K)$ forms a group under $[A]_{\sim_{\mathrm{Br}}} \cdot [B]_{\sim_{\mathrm{Br}}} = [A \otimes_K B]_{\sim_{\mathrm{Br}}}$ with neutral element $[K]_{\sim_{\mathrm{Br}}}$ where $A, B \in \mathsf{CSA}$ and $[A]^{-1}_{\sim_{Br}} = [A^{\mathrm{opp}}]_{\sim_{\mathrm{Br}}}$. We need to prove the following properties:

1. associativity: for all $A, B, C \in \mathsf{CSA}$, $[A]_{\sim_{\mathrm{Br}}} \cdot ([B]_{\sim_{\mathrm{Br}}} \cdot [C]_{\sim_{\mathrm{Br}}}) = ([A]_{\sim_{\mathrm{Br}}} \cdot [B]_{\sim_{\mathrm{Br}}}) \cdot [C]_{\sim_{\mathrm{Br}}}$ because $A \otimes_R (B \otimes_R C) \cong (A \otimes_R B) \otimes_R C$ as K-algebras.

2. neutral element: for all $A \in \mathsf{CSA}$, $[K]_{\sim_{\mathrm{Br}}} \cdot [A]_{\sim_{\mathrm{Br}}} = [A]_{\sim_{\mathrm{Br}}} = [A]_{\sim_{\mathrm{Br}}} \cdot [K]_{\sim_{\mathrm{Br}}}$. Since $[K]_{\sim_{\mathrm{Br}}} \cdot [A]_{\sim_{\mathrm{Br}}} = [K \otimes_K A]_{\sim_{\mathrm{Br}}}$, in construction 3.1.4, we see that $\mathrm{Mat}_n(A) \cong A \otimes_K \mathrm{Mat}_n(K)$, by lemma 4.1.6, $A \otimes_K \mathrm{Mat}_n(K)$ is Brauer equivalent to $A \otimes_K K$ since $K \sim_{\mathrm{Br}} \mathrm{Mat}_n(K)$.

3. cancellation: for all $A \in \mathsf{CSA}$, we need $[A]_{\sim_{\mathrm{Br}}} \cdot [A^{\mathrm{opp}}]_{\sim_{\mathrm{Br}}}$, that is we want $A \otimes_K A^{\mathrm{opp}} \sim_{\mathrm{Br}} K$. By construction 3.1.1, we have $A \otimes_K A^{\mathrm{opp}} \cong \mathrm{End}_K A$ which is isomorphic to $\mathrm{Mat}_{\dim_K A}(K)$ as K-algebras.

Theorem 4.1.7. If K is algebraically closed, $\mathrm{Br}(K)$ is trivial; in particular $\mathrm{Br}_n(\mathbb{C})$ is trivial.

Proof. We need to show that every $A \in \mathsf{CSA}$ is isomorphic to $\mathrm{Mat}_n(K)$ for some K when K is algebraically closed. Indeed, by theorem 3.2.6, $A \cong \mathrm{Mat}_n(D)$ for some division algebra D and $n \in \mathbb{N}_{\geqslant 0}$. Since K is algebraically closed and D is an integral domain and finite dimensional, the structure morphism $\rho : K \to D$ is a isomorphism; therefore $A \cong \mathrm{Mat}_n(K)$. □

Lemma 4.1.8. Let $A, B \in \mathsf{CSA}_K$. There exists a division K-algebra D and non-zero $m, n \in \mathbb{N}$ such that $A \cong \mathrm{Mat}_m(D)$ and $B \cong \mathrm{Mat}_n(D)$ as K-algebras.

Proof. By theorem 3.2.6, we can find division algebras S_A, S_B and non-zero $m, n \in \mathbb{N}$ such that $A \cong \mathrm{Mat}_n(S_A)$ and $B \cong \mathrm{Mat}_m(S_B)$ as K-algebras. Hence $B \sim_{\mathrm{Br}} A \sim_{\mathrm{Br}} \mathrm{Mat}_n(S_A) \sim_{\mathrm{Br}} S_A$, in another word, for some non-zero $a, a' \in \mathbb{N}$, we have $\mathrm{Mat}_a(B) \cong \mathrm{Mat}_{a'}(S_A)$ as K-algebras. Hence, by theorem 3.2.7, we have that $S_A \cong S_B$ as K-algebras and the lemma is proved. □

4.2 Base Change

In this section let E/K be a field extension. We have seen in corollary 1.1.11 that if $A \in \mathsf{CSA}_K$ then $E \otimes_K A \in \mathsf{CSA}_E$; therefore we have a set-theoretic function $\mathsf{CSA}_K \to \mathsf{CSA}_E$. In this section we prove that this descends to a group homomorphism $\mathrm{Br}(K) \to \mathrm{Br}(E)$. For brevity, if $A \in \mathsf{CSA}_K$, we denote $E \otimes_K A$ as A_E when this causes no confusion.

Construction 4.2.1. We will construct a series of isomorphisms (either over K or E) to arrive at the conclusion that $A \sim_{\mathrm{Br}_K} B$ implies $A_E \sim_{\mathrm{Br}_E} B_E$. Assume $m, n \in \mathbb{N}_{\geqslant 0}$ are such that $\mathrm{Mat}_m(A) \cong \mathrm{Mat}_n(B)$ are K-algebras. Then we do the following calculation: as E-algebras

$$
\begin{aligned}
\mathrm{Mat}_m(A_E) &\cong A_E \otimes_E \mathrm{Mat}_m(E) && \text{see construction 3.1.4} \\
&\cong A_E \otimes_E (E \otimes_K \mathrm{Mat}_m(K)) && \text{see } \dagger \\
&\cong E \otimes_K (A \otimes_K \mathrm{Mat}_m(K)) && \text{see } \ddagger \\
&\cong E \otimes_K \mathrm{Mat}_m(A) && \text{see construction 3.1.4 and } \dagger\dagger^{\cdot} \\
\mathrm{Mat}_n(B_E) &\cong E \otimes_K \mathrm{Mat}_n(B) && \text{same as the case of } A \\
\mathrm{Mat}_m(A_E) &\cong \mathrm{Mat}_n(B_E) && \text{see } \dagger\dagger
\end{aligned}
$$

$\dagger$: Wee need to check $\mathrm{Mat}_m(E) \cong E \otimes_K \mathrm{Mat}_m K$ as E-algebras since construction 3.1.4 only gives a K-algebra isomorphism. If $e \in E$, then its image in $E \otimes_K \mathrm{Mat}_m(K)$ is $e \otimes 1$ and its image in $\mathrm{Mat}_m(E)$ is $\mathrm{diag}(e)$ which under the K-algebra isomorphism is mapped to $\sum_{ij} \mathrm{diag}(e)_{ij} \cdot \delta_{ij} = e \otimes 1$.
$\ddagger$: This is defined by combining two E-algebra homomorphisms

$$A_E \to A_E \otimes_K \mathrm{Mat}_m(K) \to E \otimes_K (A \otimes_K \mathrm{Mat}_m(K))$$

and

$$E \otimes_K \mathrm{Mat}_m(K) \to (E \otimes_K \mathrm{Mat}_m(K)) \otimes_K A \to E \otimes_K (A \otimes_K \mathrm{Mat}_m(K)).$$

Since $(E \otimes_K A) \otimes_E (E \otimes_K \mathrm{Mat}_m(K))$ is a simple ring, this morphism is automatically injective. It is surjective as well: let $x \in E \otimes_K (A \otimes_K \mathrm{Mat}_m(K))$, without loss of generality, assume $x = e \otimes (a \otimes \delta_{ij})$ for some $e \in E$, $a \in A$. Then precisely $(e \otimes a) \otimes (1 \otimes \delta_{ij})$ is mapped to x.
$\dagger\dagger$: a K-algebra isomorphism $A \cong B$ gives an E-algebra isomorphism $E \otimes_K A \cong E \otimes_K B$.

Thus we have a well defined function $\mathrm{Br}(K) \to \mathrm{Br}(E)$. We now check that this is a group homomorphism. $[K]_{\sim_{\mathrm{Br}_K}}$ is mapped to $[E \otimes_K K]_{\sim_{\mathrm{Br}_E}}$ but $E \otimes_K K \cong E$ as E-algebra. For $A, B \in \mathsf{CSA}_K$, we have that $[AB]_{\sim_{\mathrm{Br}_K}}$ is mapped to $(A \otimes_K B)_E \cong A_E \otimes_E B_E$ as E-algebras; hence $[AB]_{\sim_{\mathrm{Br}_K}}$ and $[A]_{\sim_{\mathrm{Br}_K}} \cdot [B]_{\sim_{\mathrm{Br}_K}}$ have the same image under base change.

Denote the base change morphism in construction 4.2.1 as Br_K^E.

Lemma 4.2.1. Br_K^K is identity.

Proof. If $A \in \mathsf{CSA}$, then $A \sim_{\mathrm{Br}} K \otimes_K A$. □

Lemma 4.2.2. Consider the tower of field extension $E/F/K$,

$$\mathrm{Br}_K^E = \mathrm{Br}_E^F \circ \mathrm{Br}_K^E.$$

Proof. If $A \in \mathsf{CSA}_K$, then $E \otimes_F (F \otimes_K A)$ is isomorphic to $E \otimes_F A$ as E-algebras. □

Corollary 4.2.3. Br forms a functor from category of field to category of abelian groups.

Proof. This is the categorical version of lemma 4.2.1 and lemma 4.2.2. □

Definition 4.2.2 (Relative Brauer Group). Let E/K be a field extension, we define the relative Brauer group $\mathrm{Br}(E/K)$ to be the kernel of the base change morphism Br_K^E.

Remark 4.2.4. Unpacking the definition of the relative Brauer group, we see that for any $A \in \mathsf{CSA}_K$, if $E \otimes_K A \cong \mathrm{Mat}_n(E)$ as E-algebras, then $\mathrm{Br}_K^E([A]_{\sim_{\mathrm{Br}}}) = 1$.

Definition 4.2.3 (Splitting Field). For any field extension E/K and any K-algebra A, we say E is a splitting field of A if and only if $E \otimes_K A \cong \mathrm{Mat}_n(E)$ as E-algebras for some non-zero n. We also say E splits A or A is splited by E

Theorem 4.2.5. Let E/K be a field extension and $A \in \mathsf{CSA}_K$, E splits A if and only if $[A]_{\sim_{\mathrm{Br}}} \in \mathrm{Br}(E/K)$.

Proof. The "only if" part is by definition. For the other direction, we know by definition that $\mathrm{Mat}_n(E \otimes_K A) \cong \mathrm{Mat}_m(E)$ as E-algebras for some non-zero m, n. By theorem 3.2.6, we find some division algebra D and non-zero natural number p such that $E \otimes_K A \cong \mathrm{Mat}_p(D)$ as E-algebras. Thus $\mathrm{Mat}_{pm}(E) \cong \mathrm{Mat}_{pn}(E \otimes_K A) \cong \mathrm{Mat}_{p^2 n}(D)$ as E-algebras. By theorem 3.2.7, we conclude that $E \cong D$ as E-algebras. Hence $E \otimes_K A \cong \mathrm{Mat}_p(E)$, in another word, E splits A. $\square$

Remark 4.2.6. In light of lemma 4.2.2, if K is algebraic closed then K splits any K-algebra A. Indeed, K splits A if and only if $[A]_{\sim_{\mathrm{Br}}}$ but $[A]_{\sim_{\mathrm{Br}}}$ is equal to 1.

Remark 4.2.7. If two CSA_K are Brauer equivalent, in another word, $A \sim_{\mathrm{Br}_K} B$, then E splits A if and only if E splits B. Indeed, if A and B are equivalent, then $[A]_{\sim_{\mathrm{Br}}} \in \mathrm{Br}(E/K)$ if and only if $[B]_{\sim_{\mathrm{Br}}} \in \mathrm{Br}(E/K)$.

4.3 Good Representative Lemma

In this section, let K/F be a finite dimensional field extension.

Lemma 4.3.1. Let $A \in \mathsf{CSA}_F$ splitted by K. There exists a $B \in \mathsf{CSA}_F$ such that

- $[A]_{\sim_{\mathrm{Br}}}[B]_{\sim_{\mathrm{Br}}} = 1$
- there exists F-algebra map $K \hookrightarrow B$
- $(\dim_F K)^2 = \dim_F B$.

Proof. Since K splits A, we find a non-zero natural number n such that $K \otimes_F A \cong \mathrm{Mat}_n K \cong \mathrm{End}_K(K^n)$ as K-algebras. We define an F-algebra map $\iota : A \to \mathrm{End}_F(K^n)$ by

$$A \longrightarrow K \otimes_F A \xrightarrow{\cong} \mathrm{End}_K(K^n) \xrightarrow{|_F} \mathrm{End}_F(K^n) \ ,$$

where $|_F$ is restriction of scalars. Since A is simple, ι is injective, therefore $A \cong \iota(A)$ as F-algebras. Define B as $C_{\mathrm{End}_F(K^n)}(\iota(A))$, the centralizer of the range of ι in $\mathrm{End}_F(K^n)$. We construct an embedding $K \hookrightarrow B$ by $r \mapsto (r \cdot \bullet)$

B is a central F-algebra: if $x \in Z(B)$, then $x \in \iota(A)$ because by theorem 3.4.13, it is sufficient to prove that x is in $C_{\mathrm{End}_F(K^n)}(B)$ which follows from the fact that $x \in Z(B)$. In fact, $x \in Z(\iota(A))$: suppose $a \in A$, we need to check $x \cdot \iota(a) = \iota(a) \cdot x$, this is the case because B is defined as the centralizer of $\iota(A)$. Since $\iota(A) \cong A$ as F-algebras, $\iota(A)$ is F-central, hence $x \in F$.

B is a simple ring: by lemma 3.4.10, it is sufficient to prove that $\iota(A)$ is a simple ring which comes from $A \cong \iota(A)$ as F-algebras.

By corollary 3.4.12, we have F-algebra isomorphism $\mathrm{End}_F(K^n) \cong \iota(A) \otimes_F B \cong A \otimes_F B$. Since $\mathrm{End}_F(K^n) \cong \mathrm{Mat}_{\dim_F(K^n)}(F)$ as F-algebras, we see that $[A]_{\sim_{\mathrm{Br}}}$ and $[B]_{\sim_{\mathrm{Br}}}$ are inverses.

By lemma 3.4.11, $\dim_F B \cdot \dim_F \iota(A) = \dim_F B \cdot \dim_F A = \dim_F \mathrm{End}_F(K^n) = (\dim_F(K^n))^2 = (\dim_F K \cdot \dim_K(K^n))^2 = n^2 \cdot (\dim_F K)^2$. On the other hand, since $K \otimes_F A \cong \mathrm{Mat}_n K$, we have $\dim_F K \otimes_F A = \dim_F K \cdot \dim_F A = \dim_F \mathrm{Mat}_n K = \dim_F K \dim_K \mathrm{Mat}_n K = n^2 \dim_F K$. Since $\dim_F K \neq 0$, we conclude $\dim_F A = n^2$. Since $n \neq 0$ and $\dim_F(B) \cdot \dim_F(A) = n^2 \dim_F(B) = n^2(\dim_F K)^2$, we get the desired result.

□

Corollary 4.3.2. Let $A \in \mathsf{CSA}_F$ splitted by K. There exists a $B \in \mathsf{CSA}_F$ such that

- $[B]_{\sim_{\mathrm{Br}}} = [A]_{\sim_{\mathrm{Br}}}$
- there exists an F-algebra map $K \hookrightarrow B$
- $(\dim_F K)^2 = \dim_F B$.

Proof. Let B and $\iota : K \hookrightarrow B$ be as in lemma 4.3.1. Consider B^{opp} and $K \hookrightarrow B \to B^{\mathrm{opp}}$. This works. □

Theorem 4.3.3. Let $A \in \mathsf{CSA}_F$. K splits A if and only if there exists a $B \in \mathsf{CSA}_F$ such that

- $[B]_{\sim_{\mathrm{Br}}} = [A]_{\sim_{\mathrm{Br}}}$
- there exists an F-algebra map $K \hookrightarrow B$
- $(\dim_F K)^2 = \dim_F B$.

Proof. The "if" direction is corollary 4.3.2. For the "only if" direction, let $B \in \mathsf{CSA}_F$ and $\iota : K \hookrightarrow B$ be given. We give B a K-module structure by right multiplication, that is for any $a \in K$ and $b \in B$, we define $a \cdot b := b \cdot \iota(a)$. Since B is a finite dimensional F-vector space and K/F is a finite dimensional field extension, B is a finite dimensional K-vector space as well. Since $[B]_{\sim_{\mathrm{Br}}} = [A]_{\sim_{\mathrm{Br}}}$, it is sufficient to show that K splits B. We define an F-bilinear map $\mu : K \to B \to \mathrm{End}_K B$ by $(c, a) \mapsto (c \cdot a \cdot \bullet)$ which induce an F-linear map $\mu' : K \otimes_F B \to \mathrm{End}_K B$. Since for any $r, c \in K$ and $a \in B$, we have $\mu'(r \cdot c \otimes a)(a') = aa'\iota(rc) = aa'\iota(c)\iota(r) = r \cdot \mu'(c \otimes a)$, that is μ' is K-linear as well. Note that

$$\mu'(1) = \mu'(1 \otimes 1) = (1 \cdot 1 \cdot \bullet) = 1$$

and that

$$\begin{aligned}
\mu'(c \otimes a \cdot c' \otimes a')(a'') &= \mu'(cc' \otimes aa')(a'') \\
&= cc' \cdot aa' \cdot a'' \\
&= aa'a''\iota(cc') \\
&= a(a'a''\iota(c'))\iota(c) \\
&= \mu'(c \otimes a)(a'a''\iota(c')) \\
&= \mu'(c \otimes a)\left(\mu'(c' \otimes a')(a'')\right) \\
&= \left(\mu'(c \otimes a) \circ \mu'(c' \otimes a')\right)(a'')
\end{aligned},$$

that is, μ' is an K-algebra map.

If we can show that μ' is a bijection, we will prove the result for $K \otimes_F B \cong \mathrm{End}_K B \cong \mathrm{Mat}_{\dim_K B} K$ as K-algebras. By corollary 1.1.8, it is sufficient to show $\dim_K K \otimes_F B = \dim_K \mathrm{End}_K B$.

Let n denote $\dim_F K$. Since, $\dim_F K \dim_K K \otimes_F B = \dim_F K \otimes_F B = \dim_F K \dim_F B$. we have $\dim_K K \otimes_F B = \dim_F B = (\dim_F K)^2$. On the other hand, since $(\dim_F K)^2 = \dim_F B = \dim_F K \dim_K B$, we have $\dim_K B = \dim_F K$; thus $\dim_K \mathrm{End}_K B = (\dim_K B)^2 = (\dim_F K)^2$ and the result is proved. □

In light of theorem 4.3.3, we isolate the following useful definition:

Definition 4.3.1 (Good Representation). For any $X \in \mathrm{Br}(F)$, a K-good representation of X is an $A \in \mathsf{CSA}_F$ and an F-algebra map $K \hookrightarrow A$ such that $[A]_{\sim_{\mathrm{Br}}} = X$ and $\dim_F A = (\dim_F K)^2$. We often denote the F-algebra map $K \hookrightarrow A$ as ι or ι_A.

When K is clear from context, we will simply say good representation instead of K-good representation

Corollary 4.3.4. For any $X \in \mathrm{Br}(F)$, $X \in \mathrm{Br}(K/F)$ if and only if X admits a good representation.

Proof. Rephrase of theorem 4.3.3 and theorem 4.2.5. □

4.3.1 Basic Properties

We observe the following easy result about good representations. Let $X \in \mathrm{Br}(F)$ and A be a good representation of X.

Lemma 4.3.5. The range $\iota_A(A)$ is a simple ring.

Proof. Because K is a simple ring, ι_A is injective therefore $\iota_A(A) \cong K$. □

Lemma 4.3.6. $C_A(\iota_A(A)) = \iota_A(A)$.

Proof. In the language of section 1.2, $\iota_A(A)$ is a subfield of A, hence by lemma 1.2.3, we only need to show $\dim_F A = (\dim_F \iota_A(A))^2$. But $\dim_F A = (\dim_F K)^2$ and $\iota(A) \cong K$. □

Construction 4.3.2. We give A a K-module structure by left multiplication, that is for any $c \in K$ and $a \in A$, we define $c \cdot a$ to be $\iota_A(c)a$. Note that if $c \in F$ then $\iota_A(c)a = c \cdot a$, in another word, the K-action and the F-action on A are compatible. Then A is a finite dimensional K-vector space and $\dim_K A = \dim_F K$: indeed $\dim_F K \cdot \dim_K A = \dim_F K \cdot \dim_F K = \dim_F A$.

Lemma 4.3.7. If A and B are two good representations of X, then $A \cong B$ as F-algebras.

Proof. By lemma 4.1.8, we find a division F-algebra D and non-zero natural numbers m, n such that $A \cong \mathrm{Mat}_m(D)$ and $B \cong \mathrm{Mat}_n(D)$ as F-algebras. Therefore

$$\begin{aligned}(\dim_F K)^2 = \dim_F A \quad &= m^2 \dim_F D \\ = \dim_F B \quad &= n^2 \dim_F D.\end{aligned}$$

Therefore $m = n$ and $A \cong \mathrm{Mat}_m D = \mathrm{Mat}_n D \cong B$. □

4.3.2 Conjugation Factors and Conjugation Sequences

In this section, let K/F be a field extension, $X \in \mathrm{Br}(F)$ and A be a K-good representation of X.

Remark 4.3.8. Since $\mathrm{Gal}(K/F)$ acts on $K^\star$, for $x \in K^\star$,we feel free to write $\sigma \cdot x$ when it feels more readable than $\sigma(x)$, for example when there are nested brackets.

Definition 4.3.3 (Conjugation Factor). With respect to A, a conjugation factor of σ is a unit $x_\sigma \in A^\star$ such that for all $c \in K$,

$$x_\sigma \iota_A(c) x_\sigma^{-1} = \iota_A(\sigma \cdot c).$$

A conjugation sequence is a sequence $x : \mathrm{Gal}(K/F) \to A^\star$ such that for all $\sigma \in \mathrm{Gal}(K/F)$, x_σ is a conjugation factor of σ. When we want to stress A, we say A-conjugation factor and A-conjugation sequence.

Remark 4.3.9. When x_σ is a conjugation factor of σ, the equalities $x_\sigma \iota_A(c) = x_\sigma \iota_A(\sigma(c))$ and $\iota_A(c) x_\sigma^{-1} = x_\sigma^{-1} \iota_A(\sigma(c))$ are also useful.

Construction 4.3.4. A has a conjugation sequence: let $\sigma \in \mathrm{Gal}(K/F)$, we have two F-algebra homomorphisms $K \to A$ given by ι_A and $\iota_A \circ \sigma$. Applying theorem 3.3.4 to ι_A and $\iota_A \circ \sigma$ gives us the desired conjugation factor.

Construction 4.3.5. If x is a conjugation factor of σ and y of τ, then xy is a conjugation factor of $\sigma\tau$. For any $c \in K$

$$\iota_A(\sigma \cdot \tau(c)) = x \iota_A(\tau \cdot c) x^{-1} = xy \iota_A(c) y^{-1} x^{-1} = (xy)\, \iota_A(xy)^{-1}.$$

Theorem 4.3.10. If x is an A-conjugation sequence, then $\{x_\sigma | \sigma \in \mathrm{Gal}(K/F)\}$ is an K-linearly independent set. When K/F is finite dimensional and Galois, $\{x_\sigma | \sigma \in \mathrm{Gal}(K/F)\}$ is a K-basis for A.

Proof. Suppose $\{x_\sigma\}$ is linearly dependent. Let $J \subseteq \mathrm{Gal}(K/F)$ be such that $\{x_\sigma | \sigma \in J\}$ is a maximally linearly independent subset. Then $J \neq \mathrm{Gal}(K/F)$, let $\sigma \in \mathrm{Gal}(K/F)$ be an arbitrary automorphism that is not in J. Since $\{x_\tau | \tau \in J\}$ is maximally linearly independent, $x_\sigma \in \langle x_\tau | \tau \in J \rangle$. Hence, by construction 4.3.2 we have

$$x_\sigma = \sum_{\tau \in J'} \lambda_\tau \cdot x_\tau = \sum_{\tau \in J'} \iota_A(\lambda_\tau)\, x_\tau,$$

for some non-zero $\lambda_\tau \in K$ and $J' \subseteq J$. For each $c \in K$, we have the following equality

$$\begin{aligned}
\iota_A(\sigma \cdot c)\, x_\sigma &= x_\sigma \iota_A(c) && \text{by definition 4.3.3} \\
&= \sum_{\tau \in J'} \lambda_\tau \cdot x_\tau \iota_A(c) \\
&= \sum_{\tau \in J'} \lambda_\tau \cdot \iota_A(\tau \cdot c)\, x_\tau && \text{by definition 4.3.3 again} \\
&= \sum_{\tau \in J'} \iota_A(\lambda_\tau \tau(c))\, x_\tau; \\
\iota_A(\sigma \cdot c)\, x_\sigma &= \sum_{\tau \in J'} \iota_A(\lambda_\tau)\, x_\tau \iota_A(c) \\
&= \sum_{\tau \in J'} \iota_A(\sigma(c)\lambda_\tau)\, x_\tau.
\end{aligned}$$

Since $\{x_\tau | \tau \in J'\}$ is linearly independent, we have that for each $\tau \in J'$, $\lambda_\tau \tau(c) = \sigma(c)\lambda_\tau = \lambda_\tau \sigma(c)$. Note that J' is not empty, for otherwise $x_\sigma = \sum_{\tau \in \emptyset} \lambda_\tau \cdot x_\tau = 0$ but x_σ is invertible. Since for any $\tau \in J'$, λ_τ is not zero, we have that for all $c \in K$, $\sigma(c) = \tau(c)$, i.e. $\sigma = \tau$. Hence σ is in $J' \subseteq J$ after all; contradiction.

If K/F is finite dimensional and Galois, then $\dim_F K$ is equal to the cardinality of $\mathrm{Gal}(K/F)$, then by the linear independence of $\{x_\sigma | \sigma \in \mathrm{Gal}(K/F)\}$, we conclude that it is indeed a K-basis for A. □

4.4 The Second Galois Cohomology

In this section, we construct a group isomorphism between $\mathrm{Br}(K/F) \cong \mathrm{H}^2(\mathrm{Gal}(K/F), K^\star)$ where K/F is a finite dimensional Galois extension. To keep alignment of the Brauer group, let us use the multiplicative notation for group cohomology. Recall:

Definition 4.4.1 (the Second Group Cohomology). Let G be a group and M an abelian group (written multiplicatively) with a G-action.

A function $f : G \times G \to M$ is a 2-cocycle if for all $g, h, j \in G$,

$$f(gh, j)f(g, h) = (g \cdot f(h, j))\, f(g, hj).$$

We denote the subgroup of 2-cocycles as $\mathcal{Z}^2(G, M)$.

A function $f : G \times G \to M$ is a 2-coboundary if there exists an $x : G \to M$ such that for all $g, h \in G$

$$\frac{g \cdot x(h)}{x(gh)} x(g) = f(g, h).$$

We denote the subgroup of 2-coboundaries as $\mathcal{B}^2(G, M)$.

The second group cohomology $\mathrm{H}^2(G, M)$ is defined to be the quotient group of 2-cocycles modulo 2-coboundaries ${}^{\mathcal{Z}^2(G,M)}/_{\mathcal{B}^2(G,M)}$. If $s, t \in \mathcal{Z}^2(G, M)$, we say s and t are cohomologous if their equivalence class $[s], [t] \in \mathrm{H}^2(G, M)$ are the same; in another word $st^{-1} \in \mathcal{B}^2(G, M)$.

Lemma 4.4.1. If $f \in \mathcal{B}^2(G, M)$ is a 2-cocycle and $x \in G$, we have

$$\begin{aligned} f(1, x) &= f(1, 1) \\ f(x, 1) &= x \cdot f(1, 1). \end{aligned}$$

Proof. Indeed:

$$\begin{aligned} f(1 \cdot 1, x)f(1, 1) &= (1 \cdot f(1, x))f(1, 1 \cdot x) \\ f(1, x)f(1, 1) &= f(1, x)f(1, x) \\ f(1, x) &= f(1, 1) \end{aligned}$$

and

$$\begin{aligned} f(x \cdot 1, 1)f(x, 1) &= (x \cdot f(1, 1))f(x, 1 \cdot 1) \\ f(x, 1)f(x, 1) &= (x \cdot f(1, 1))f(x, 1) \\ f(x, 1) &= x \cdot f(1, 1). \end{aligned}$$

□

In the following sections of this chapter, we assume that $X \in \mathrm{Br}(F)$ and A is a good representation of X. We use ρ, σ, τ to denote elements of $\mathrm{Gal}(K/F)$. To improve typographic aesthetics of our proofs, we sometimes use subscript to mean function application.

4.4.1 From $\mathrm{Br}(K/F)$ to $H^2(\mathrm{Gal}(K/F), K^\star)$

Lemma 4.4.2 (Twisting Conjugation Factors). If x and y are two conjugation factors of σ, then there exists a unique $c \in K$ such that $x = y\iota_A(c)$.

Proof. The uniqueness is clear: suppose $x = y\iota_A(c) = y\iota_A(c')$, then $c = c'$ because x, y are units and ι_A is injective. We first observe that $y^{-1}x \in C_A(\iota(A))$: for any $z \in K$, $y^{-1}x\iota_A(z) = y^{-1}\iota_A(\sigma(z))x = \iota_A(z)y^{-1}x$ (by remark 4.3.9). By lemma 4.3.6, $y^{-1}x \in \iota(A)$, that is for some $z \in K$, we have that $y^{-1}x = \iota_A(z)$ and the claim is proved. ☐

We denote such c by $\mathrm{twist}^\sigma(x, y)$ or $\mathrm{twist}^\sigma_{x,y}$, when σ is clear from context, we often omit the superscript. With this notation, $x = y\iota_A(\mathrm{twist}_{x,y})$.

Remark 4.4.3. $\mathrm{twist}(x, x)$ is equal to 1 by uniqueness.

Remark 4.4.4. In fact, $\mathrm{twist}(x, y)$ is in $K^\star$ and $\mathrm{twist}(x, y)^{-1} = \mathrm{twist}(y, x)$.

Lemma 4.4.5. If x and y are conjugation factors for σ, $x = \iota_A(\sigma(\mathrm{twist}_{x,y}))y$.

Proof.

$$\begin{aligned} x &= x\iota_A\left(\mathrm{twist}_{x,y}\right)x^{-1}x\iota_A(\mathrm{twist}_{y,x}) \\ &= \iota_A\left(\sigma \cdot \mathrm{twist}_{x,y}\right)x\iota_A\left(\mathrm{twist}_{y,x}\right) \\ &= \iota_A\left(\sigma \cdot \mathrm{twist}_{x,y}\right)y \end{aligned} .$$

☐

Construction 4.4.2 (Comparing Conjugation Factors). Let x be a conjugation factor for σ, y for τ and z for $\sigma\tau$. Since xy is a also a conjugation factor, we define the comparison coefficient to be $\mathrm{comp}^{\sigma,\tau}_{x,y,z} := \sigma\left(\tau\left(\mathrm{twist}_{xy,z}\right)\right)$. We often omit superscript when the context is clear. Note that $\mathrm{comp}_{x,y,z}$ is a unit in K with inverse $\sigma\left(\tau\left(\mathrm{twist}_{z,xy}\right)\right)$. By lemma 4.4.2 and lemma 4.4.5, we have the following useful equalities

$$\begin{aligned} xy &= \iota_A\left(\mathrm{comp}_{x,y,z}\right)z \\ \iota_A\left(\mathrm{comp}^{-1}_{x,y,z}\right)xy &= z \\ \iota_A\left(\mathrm{comp}_{x,y,z}\right) &= xyz^{-1} \\ \iota_A\left(\mathrm{comp}^{-1}_{x,y,z}\right) &= zy^{-1}x^{-1} \\ \ldots &= \ldots \end{aligned} .$$

Lemma 4.4.6. Let $x : \mathrm{Gal}(K/F) \to A^\star$ be a conjugation sequence. We have

$$\mathrm{comp}_{x_\rho,x_\sigma,x_{\rho\sigma}}\ \mathrm{comp}_{x_{\rho\sigma},x_\tau,x_{\rho\sigma\tau}} = \rho\left(\mathrm{comp}_{x_\sigma,x_\tau,x_{\sigma\tau}}\right)\ \mathrm{comp}_{x_\rho,x_{\sigma\tau},x_{\rho\sigma\tau}} .$$

Proof. It is sufficient to make the following calculations:

$$x_\rho\, x_\sigma x_\tau = \iota_A\left(\mathrm{comp}_{x_\rho,x_\sigma,x_{\rho\sigma}}\right)\ \iota_A\left(\mathrm{comp}_{x_{\rho\sigma},x_\tau,x_{\rho\sigma\tau}}\right)\ x_{\rho\sigma\tau} \tag{4.1}$$

$$x_\rho\left(x_\sigma x_\tau\right) = \iota_A\left(\rho \cdot \mathrm{comp}_{x_\sigma,x_\tau,x_{\sigma\tau}}\right)\ \iota_A\left(\mathrm{comp}_{x_\rho,x_{\sigma\tau},x_{\rho\sigma\tau}}\right)x_{\rho\sigma\tau} \tag{4.2}$$

Then since $x_{\rho\sigma\tau}$ is invertible and ι_A is injective, we proved the desired result.

Equation (4.1) is because: by the first equality in construction 4.4.2 (twice)

$$x_\rho x_\sigma x_\tau = \iota_A\left(\text{comp}_{x_\rho, x_\sigma, x_{\rho\sigma}}\right) x_{\rho\sigma} x_\tau = \iota_A\left(\text{comp}_{x_\rho, x_\sigma, x_{\rho\sigma}}\right) \iota_A\left(\text{comp}_{x_{\rho\sigma}, x_\tau, x_{\rho\sigma\tau}}\right) x_{\rho\sigma\tau}.$$

Equation (4.2) is because: by definition 4.3.3, we have

$$\iota_A\left(\rho \cdot \text{comp}_{x_\sigma, x_\tau, x_{\sigma\tau}}\right) x_\rho = x_\rho \iota_A\left(\text{comp}_{x_\sigma, x_\tau, x_{\sigma\tau}}\right),$$

therefore by construction 4.2.1

$$\begin{aligned} x_\rho\left(x_\sigma x_\tau\right) &= x_\rho \iota_A\left(\text{comp}_{x_\sigma, x_\tau, x_{\sigma\tau}}\right) x_{\sigma\tau} \\ &= \iota_A\left(\rho \cdot \text{comp}_{x_\sigma, x_\tau, x_{\sigma\tau}}\right) x_\rho x_{\sigma\tau} \\ &= \iota_A\left(\rho \cdot \text{comp}_{x_\sigma, x_\tau, x_{\sigma\tau}}\right) \iota_A\left(\text{comp}_{x_\rho, x_{\sigma\tau}, x_{\rho\sigma\tau}}\right) x_{\rho\sigma\tau} \end{aligned}.$$

□

Construction 4.4.3 (from good representation to 2-cocycle). Let x be an A-conjugation sequence. We associate with x a function $\mathcal{B}^2(x) : \text{Gal}(K/F) \times \text{Gal}(K/F) \to K^\star$ defined by

$$(\sigma, \tau) \mapsto \text{comp}_{x_\sigma, x_\tau, x_{\sigma\tau}}.$$

We will write $\mathcal{B}^2(x)$ as $\mathcal{B}^2_{A,x}$, $\mathcal{B}^2_A(x)$ or $\mathcal{B}^2_x$ as well.

Lemma 4.4.7. For any A-conjugation sequence x, $\mathcal{B}^2_x \in \mathcal{B}^2\left(\text{Gal}(K/F), K^\star\right)$, that is $\mathcal{B}_x$ is indeed a 2-cocycle.

Proof. We need to prove

$$\mathcal{B}_x(\rho\sigma, \tau)\,\mathcal{B}_x(\rho, \sigma) = \rho\left(\mathcal{B}_x(\sigma, \tau)\right)\,\mathcal{B}_x(\rho, \sigma\tau).$$

But this is exactly lemma 4.4.6. □

For any good representation A of $X \in \text{Br}(K/F)$ and any A-conjugation sequence x, we have constructed a 2-cocycle $\mathcal{B}^2_A(x)$. But to obtain a well-defined function from $\text{Br}(K/F)$ to $H^2\left(\text{Gal}(K/F), K^\star\right)$, we need to verify that for any other good representation B of X and B-conjugation sequence y, $\mathcal{B}^2_A(x)$ and $\mathcal{B}^2_B(y)$ are cohomologous. Let us fix another good representation B of $X \in \text{Br}(K/F)$ and a B-conjugation sequence y.

Construction 4.4.4. By lemma 4.3.7, A and B are isomorphic as F-algebras, we use $e_{A,B}$ to denote an arbitrary F-algebra isomorphism between A and B. When there is no confusion, we write e instead of $e_{A,B}$ Since $e \circ \iota_A$ and ι_B are two F-algebra homomorphism from K to B, by theorem 3.3.4, there exists some $u \in B^\star$ such that for all $r \in K$, we have $\iota_B(r) = ue\left(\iota_A(r)\right)u^{-1}$ (or equivalently, $u^{-1}\iota_B(r)u = e\left(\iota_A(r)\right)$). When there is confusion, we write $u_{A,B}$ instead of u.

Lemma 4.4.8. For any $c \in K$, $\sigma \in \text{Gal}(K/F)$ and A-conjugation factor x of σ, we have

$$\iota_B(\sigma \cdot c) = ue(x)u^{-1}\,\iota_B(c)\,ue\left(x^{-1}\right)u^{-1}.$$

Proof. From definition 4.3.3, we have $e(\iota_A(\sigma \cdot c)) = e\left(x\iota_A(c)x^{-1}\right)$. Substituting it in construction 4.4.4, we get

$$\begin{aligned}\iota_B(\sigma \cdot c) &= ue\left(x\iota_A(c)x^{-1}\right)u^{-1}\\ &= ue(x)e(\iota_A(c))\,e\left(x^{-1}\right)u^{-1}\\ &= ue(x)u^{-1}\iota_B(c)ue\left(x^{-1}\right)u^{-1}.\end{aligned}$$

□

Construction 4.4.5. If x is an A-conjugation factor for σ, we can obtain a B-conjugation factor for σ by defining $B_\star x := ue(x)u^{-1}$ with inverse $ue\left(x^{-1}\right)u^{-1}$. We use lemma 4.4.8 to check that $B_\star x$ is indeed a conjugation factor for σ. If y is a B-conjugation factor for σ, another useful constant is $\nu := \sigma\left(\mathrm{twist}_{y,B_\star x}\right)$. We have

$$\begin{aligned}y &= \iota_B(\nu)\; B_\star x\\ \iota_B(\nu) &= ue(\iota_A(\nu))\,u^{-1}.\\ \nu^{-1} &= \sigma\left(\mathrm{twist}_{B_\star x,y}\right)\end{aligned}$$

We also write $\nu_{x,y}$ or even $\nu^{A,B}_{x,y}$ when we stress the importance of good representation A and B and their conjugation factor x and y.

Lemma 4.4.9. Let x be an A-conjugation sequence and y a B-conjugation sequence. We have

$$\mathrm{comp}_{y_\sigma,y_\tau,y_{\sigma\tau}}\,\nu_{x_{\sigma\tau},y_{\sigma\tau}} = \nu_{x_\sigma,y_\sigma}\,\sigma\left(\nu_{x_\tau,y_\tau}\right)\mathrm{comp}_{x_\sigma,x_\tau,x_{\sigma\tau}}\,.$$

Proof. By construction 4.4.2, we have $y_\sigma y_\tau = \iota_B\left(\mathrm{comp}_{y_\sigma,y_\tau,y_{\sigma\tau}}\right)y_{\sigma\tau}$. By repeated application of construction 4.4.5 and construction 4.4.4, we have

$$\begin{aligned}y_{\sigma\tau} &= u\,e\left(\iota_A\left(\nu_{x_{\sigma\tau},y_{\sigma\tau}}\right)x_{\sigma\tau}\right)u^{-1}\\ y_\sigma y_\tau &= u\,e\left(\iota_A\left(\nu_{x_\sigma,y_\sigma}\right)x_\sigma\iota_A\left(\nu_{x_\tau,y_\tau}\right)x_\tau\right)u^{-1}\\ &= \iota_B\left(\mathrm{comp}_{y_\sigma,y_\tau,y_{\sigma\tau}}\right)y_{\sigma\tau}\\ &= \iota_B\left(\mathrm{comp}_{y_\sigma,y_\tau,y_{\sigma\tau}}\right)u\,e\left(\iota_A\left(\nu_{x_{\sigma\tau},y_{\sigma\tau}}\right)x_{\sigma\tau}\right)u^{-1}\\ &= u\,e\left(\iota_A\left(\mathrm{comp}_{y_\sigma,y_\tau,y_{\sigma\tau}}\right)\right)u^{-1}\;\;ue\left(\iota_A\left(\nu_{x_{\sigma\tau},y_{\sigma\tau}}\right)x_{\sigma\tau}\right)u^{-1}\\ &= ue\left(\iota_A\left(\mathrm{comp}_{y_\sigma,y_\tau,y_{\sigma\tau}}\,\nu_{x_{\sigma\tau},y_{\sigma\tau}}\right)x_{\sigma\tau}\right)u^{-1}.\end{aligned}$$

Hence

$$\iota_A\left(\nu_{x_\sigma,y_\sigma}\right)x_\sigma\iota_A\left(\nu_{x_\tau,y_\tau}\right)x_\tau = \iota_A\left(\mathrm{comp}_{y_\sigma,y_\tau,y_{\sigma\tau}}\,\nu_{x_{\sigma\tau},y_{\sigma\tau}}\right)x_{\sigma\tau}.$$

We also have by definition 4.3.3

$$x_\sigma\iota_A\left(\nu_{x_\tau,y_\tau}\right)x_\tau = \iota_A\left(\sigma\cdot\nu_{x_\tau y_\tau}\right)x_\sigma x_\tau.$$

Hence

$$\begin{aligned}\iota_A\left(\nu_{x_\sigma,y_\sigma}\right)x_\sigma\iota_A\left(\nu_{x_\tau,y_\tau}\right)x_\tau &= \iota_A\left(\nu_{x_\sigma,y_\sigma}\,\sigma\left(\nu_{x_\tau,y_\tau}\right)\right)x_\sigma x_\tau\\ &= \iota_A\left(\nu_{x_\sigma,y_\sigma}\,\sigma\left(\nu_{x_\tau,y_\tau}\right)\mathrm{comp}_{x_\sigma,x_\tau,x_{\sigma\tau}}\right)x_{\sigma\tau}\\ &= \iota_A\left(\mathrm{comp}_{y_\sigma,y_\tau,y_{\sigma\tau}}\,\nu_{x_{\sigma\tau},y_{\sigma\tau}}\right)x_{\sigma\tau}.\end{aligned}$$

Cancelling $x_{\sigma\tau}$ and by injectivity of ι_A, the result is proved. □

Lemma 4.4.10. Let x be an A-conjugation sequence and y a B-conjugation sequence. We have

$$\mathcal{B}^2_{B,y}(\sigma,\tau)\nu_{x_{\sigma\tau},y_{\sigma\tau}} = \nu_{x_\sigma,y_\sigma}\,\sigma\left(\nu_{x_\tau,y_\tau}\right)\mathcal{B}^2_{A,y}(\sigma,\tau).$$

Proof. If we unfold construction 4.4.3, we discover the lemma is saying exactly lemma 4.4.9. □

We finally arrive at our main conclusion for this section.

Corollary 4.4.11. Let x be an A-conjugation sequence and y a B-conjugation sequence. $\mathcal{B}^2_{A,x}$ and $\mathcal{B}^2_{B,y}$ are 2-cohomologous.

Proof. By definition 4.4.1, we need to find a function $f : \mathrm{Gal}(K/F) \to K^\star$ such that for all $\sigma, \tau \in \mathrm{Gal}(K/F)$,

$$\frac{\sigma\left(f(\tau)\right)}{f\left(\sigma\tau\right)} f(\sigma) = \frac{\mathcal{B}^2_{B,y}}{\mathcal{B}^2_{A,x}}.$$

Let $f(\rho) := \nu_{x_\rho,y_\rho}$, by lemma 4.4.10 we see the equality holds. □

Construction 4.4.6 (from $\mathrm{Br}(K/F)$ to $H^2\left(\mathrm{Gal}(K/F), K^\star\right)$). Let $X \in \mathrm{Br}(K/F)$, by corollary 4.3.4, X admits a good representation A; by construction 4.3.4, A admits a conjugation sequence x. We associate with X an element $H^2(X) := \left[\mathcal{B}^2_{A,x}\right]$in $H^2\left(\mathrm{Gal}(K/F), K^\star\right)$. By corollary 4.4.11, for any other good representation B and B-conjugation sequence y, we have $\left[\mathcal{B}^2_{A,x}\right] = \left[\mathcal{B}^2_{B,y}\right]$, hence we have a well-defined function $H^2 : \mathrm{Br}(K/F) \to H^2\left(\mathrm{Gal}(K/F), K^\star\right)$.

4.4.2 Cross Product as a Central Simple Algebra

Let $\mathfrak{a} \in \mathcal{B}^2\left(\mathrm{Gal}(K/F), K^\star\right)$ be any 2-cocycle. In this section, we construct the cross product associated with $\mathfrak{a}$ which we prove to be F-central simple. Finally, we show that if $\mathfrak{a}, \mathfrak{b} \in \mathcal{B}^2\left(\mathrm{Gal}(K/F), K^\star\right)$ are cohomologous, the cross products associated with $\mathfrak{a}$ and $\mathfrak{b}$ are Brauer equivalent.

Construction 4.4.7 (Cross product). Denote $\mathfrak{C}_\mathfrak{a}$ to be $\mathrm{Gal}(K/F) \to K$, i.e. functions from $\mathrm{Gal}(K/F)$ to K. Notationally, elements of $\mathfrak{C}_\mathfrak{a}$ are sequences in K indexed by $\mathrm{Gal}(K/F)$; we denote $\Delta^\mathfrak{a}_{\sigma,c}$ to be the sequence with value c at σ-th index and zero elsewhere. When $\mathfrak{a}$ is clear from context, we will omit the superscript. We give $\mathfrak{C}_\mathfrak{a}$ the usual zero, addition, negation, that is, we give $\mathfrak{C}_\mathfrak{a}$ the normal additive abelian group structure. Since for each $c \in \mathfrak{C}_\mathfrak{a}$,

$$c = \sum_{\sigma \in \mathrm{Gal}(K/F)} \Delta_{\sigma,c(\sigma)},$$

it is often, if not always, sufficient to consider the special cases of $\Delta_{\sigma,c}$ and extend the result linearly. For multiplications, we define the result of multiplying $\Delta_{\sigma,c}, \Delta_{\tau,d}\ \mathfrak{C}_\mathfrak{a}$ to be $\Delta_{\sigma\tau, c\sigma(d)\,\mathfrak{a}(\sigma,\tau)}$. Immediately, if either c or d is 0, the result of multiplication is also zero. That is, for all $c \in \mathfrak{C}_\mathfrak{a}$, we have $c \cdot 0 = 0 \cdot c = 0$. For any $r \in F$ and $\Delta_{\sigma,c} \in \mathfrak{C}_\mathfrak{a}$, we define $r \cdot \Delta_{\sigma,c}$ to be $\Delta_{\sigma,r\cdot c}$.

Remark 4.4.12. When K/F is infinite dimensional, the correct definition of $\mathfrak{C}_\mathfrak{a}$ is perhaps $\bigoplus_{\sigma \in \mathrm{Gal}(K/F)} K$. But in Lean4, function type is easier to manipulate than direct sums. Since our scope is finite dimensional Galois extension, our definition is still accurate.

Lemma 4.4.13. The cross product $\mathfrak{C}_\mathfrak{a}$ is a ring with the multiplicative unit $\Delta_{\mathrm{id},\mathfrak{a}(\mathrm{id},\mathrm{id})^{-1}}$. The F-action on $\mathfrak{C}_\mathfrak{a}$ defined by $r \cdot \Delta_{\sigma,c} := \Delta_{\sigma,r\cdot c}$ makes it an F-algebra.

Proof. We verify the axioms of rings on elements of the form $\Delta_{\sigma,c}$. Let $\sigma, \tau, \rho \in \mathrm{Gal}(K/F)$ and $a, b, c \in K$.

- associativity of multiplication. We need to check that $\Delta_{\sigma,a}\left(\Delta_{\tau,b}\Delta_{\rho,c}\right) = \left(\Delta_{\sigma,a}\Delta_{\tau,b}\right)\Delta_{\rho,c}$:

$$\begin{aligned}\Delta_{\sigma,a}\left(\Delta_{\tau,b}\Delta_{\rho,c}\right) &= \Delta_{\sigma,a}\Delta_{\tau\rho,b\tau(c)a(\sigma,\tau)}\\ &= \Delta_{\sigma\tau\rho,a\sigma(b)\sigma(\tau(c))\sigma(a(\sigma,\tau))};\\ \left(\Delta_{\sigma,a}\Delta_{\tau,b}\right)\Delta_{\rho,c} &= \Delta_{\sigma\tau,a\sigma(b)a(\sigma,\tau)}\Delta_{\rho,c}\\ &= \Delta_{\sigma\tau\rho,a\sigma(b)a(\sigma,\tau)\sigma(\tau(c))a(\sigma\tau,\rho)}.\end{aligned}$$

  Hence it is sufficient to check

$$\sigma(\tau(c))\sigma(a(\sigma,\tau)) = a(\sigma,\tau)\sigma(\tau(c))a(\sigma\tau,\rho).$$

  This is the 2-cocycle condition in definition 4.4.1 (modulo commutativity of K).

- multiplicative unit: we need to check $\Delta_{\sigma,a}\Delta_{\mathrm{id},a(\mathrm{id},\mathrm{id})} = \Delta_{\mathrm{id},a(\mathrm{id},\mathrm{id})}\Delta_{\sigma,a} = \Delta_{\sigma,a}$. By multiple applications of lemma 4.4.1

$$\begin{aligned}\Delta_{\mathrm{id},a(\mathrm{id},\mathrm{id})^{-1}}\Delta_{\sigma,a} &= \Delta_{\sigma,a(\mathrm{id},\mathrm{id})^{-1}a a(\mathrm{id},\sigma)}\\ &= \Delta_{\sigma,a(\mathrm{id},\mathrm{id})a a(\mathrm{id},\mathrm{id})}\\ &= \Delta_{\sigma,a}\\ \Delta_{\sigma,a}\Delta_{\mathrm{id},a(\mathrm{id},\mathrm{id})^{-1}} &= \Delta_{\sigma,a\sigma(a(\mathrm{id},\mathrm{id}))^{-1}a(\sigma,\mathrm{id})}\\ &= \Delta_{\sigma,a\sigma(a(\mathrm{id},\mathrm{id}))^{-1}\sigma(a(\mathrm{id},\mathrm{id}))}\\ &= \Delta_{\sigma,a}\end{aligned}$$

- distributivity: We need to check left-distributivity $\Delta_{\sigma,a}\left(\Delta_{\tau,b}+\Delta_{\rho,c}\right) = \Delta_{\sigma,a}\Delta_{\tau,b}+\Delta_{\sigma,a}\Delta_{\rho,c}$ and right distributivity $\left(\Delta_{\tau,b}+\Delta_{\rho,c}\right)\Delta_{\sigma,a} = \Delta_{\tau,b}\Delta_{\sigma,a}+\Delta_{\rho,c}\Delta_{\sigma,a}$. This is precisely what "extend linearly" means.

- F-algebra: We need to check for all $r \in F$, $\left(r \cdot \Delta_{\mathrm{id},a(\mathrm{id},\mathrm{id})^{-1}}\right)\Delta_{\sigma,c} = \Delta_{\sigma,c}\left(r \cdot \Delta_{\mathrm{id},a(\mathrm{id},\mathrm{id})^{-1}}\right)$. By lemma 4.4.1

$$\begin{aligned}\left(r \cdot \Delta_{\mathrm{id},a(\mathrm{id},\mathrm{id})^{-1}}\right)\Delta_{\sigma,c} &= \Delta_{\mathrm{id},r\cdot a(\mathrm{id},\mathrm{id})^{-1}}\Delta_{\sigma,c}\\ &= \Delta_{\sigma,(r\cdot a(\mathrm{id},\mathrm{id})^{-1})c a(\mathrm{id},\sigma)}\\ &= \Delta_{\sigma,(r\cdot a(\mathrm{id},\mathrm{id})^{-1})c a(\mathrm{id},\mathrm{id})}\\ &= \Delta_{\sigma,r\cdot c}\\ \Delta_{\sigma,c}\left(r \cdot \Delta_{\mathrm{id},a(\mathrm{id},\mathrm{id})^{-1}}\right) &= \Delta_{\sigma,c}\Delta_{\mathrm{id},r\cdot a(\mathrm{id},\mathrm{id})^{-1}}\\ &= \Delta_{\sigma,c\sigma(r\cdot a(\mathrm{id},\mathrm{id})^{-1})a(\sigma,\mathrm{id})}\\ &= \Delta_{\sigma,c(r\cdot\sigma(a(\mathrm{id},\mathrm{id})^{-1}))a(\mathrm{id},\mathrm{id})^{-1}}\\ &= \Delta_{\sigma,c(r\cdot 1)}\\ &= \Delta_{\sigma,r\cdot c}.\end{aligned}$$

□

From now on, we feel free to write $1 \in \mathfrak{C}_a$ instead of $\Delta_{\mathrm{id},a(\mathrm{id},\mathrm{id})^{-1}}$. Then the algebra map $F \hookrightarrow \mathfrak{C}_a$ is the map $r \mapsto r \cdot 1$.

Construction 4.4.8 (K-embedding). The map $\iota_{\mathfrak{C}_a} : K \to \mathfrak{C}_a$ defined by

$$b \mapsto \Delta_{\mathrm{id},\, b a(\mathrm{id},\mathrm{id})^{-1}}$$

is an F-algebra map. Checking that $\iota_{\mathfrak{C}_a}$ preserves 1, multiplication and addition uses nothing but axioms of ring. For any $r \in F$, we need to check $\iota_{\mathfrak{C}_a}(r) = r \cdot 1$. Indeed $\iota_{\mathfrak{C}_a}(r) = \Delta_{\mathrm{id}, r \cdot a(\mathrm{id},\mathrm{id})^{-1}}$ and $r \cdot 1 = r \cdot \Delta_{\mathrm{id},a(\mathrm{id},\mathrm{id})^{-1}} = \Delta_{\mathrm{id}, r\cdot a(\mathrm{id},\mathrm{id})^{-1}}$. When the context is clear, we also write ι_a instead of $\iota_{\mathfrak{C}_a}$. We give $\mathfrak{C}_a$ a K-module structure by left-multiplication, that is for any $b \in K$ and $c \in \mathfrak{C}_a$, we define $b \cdot c := \iota_a(b)c$.

We note the following useful equality: for any $b \in K$

$$b \cdot \Delta_{\sigma,c} = \iota_a(b)\Delta_{\sigma,c} = \Delta_{\sigma,bc},$$

indeed: $\iota_a(b)\Delta_{\sigma,c} = \Delta_{\mathrm{id},ba(\mathrm{id},\mathrm{id})^{-1}}\Delta_{\sigma,c} = \Delta_{\sigma,ba(\mathrm{id},\mathrm{id})^{-1}ca(\mathrm{id},\sigma)} = \Delta_{\sigma,ba(\mathrm{id},\mathrm{id})^{-1}ca(\mathrm{id},\mathrm{id})} = \Delta_{\sigma,bc}$ by lemma 4.4.1. In another word, for any $b \in F$ and $c \in \mathfrak{C}_a$, the K-action of b on c and the F-action of b on c agree.

Lemma 4.4.14. For every $\sigma \in \mathrm{Gal}(K/F)$, $\Delta_{\sigma,1}$ is invertible.

Proof. It is sufficient to prove that $\Delta_{\sigma,1}$ has a left inverse and right inverse. The left inverse of $\Delta_{\sigma,1}$ is

$$\Delta_{\sigma^{-1},a(\sigma^{-1},\sigma)^{-1}a(\mathrm{id},\mathrm{id})^{-1}}.$$

Indeed, for any $a \in K$, we have

$$\Delta_{\sigma^{-1},a}\,\Delta_{\sigma,1} = \Delta_{\mathrm{id},aa(\sigma^{-1},\sigma)},$$

hence substitute $a = a\left(\sigma^{-1},\sigma\right)^{-1} a(\mathrm{id},\mathrm{id})^{-1}$, we see the right hand side is $\Delta_{\mathrm{id},a(\mathrm{id},\mathrm{id})^{-1}}$ which is precisely $1 \in \mathfrak{C}_a$. The right inverse is

$$\Delta_{\sigma^{-1},\sigma^{-1}\left(a(\sigma,\sigma^{-1})^{-1}a(\mathrm{id},\mathrm{id})^{-1}\right)}.$$

Indeed, for any $a \in K$, we have

$$\Delta_{\sigma,1}\,\Delta_{\sigma^{-1},a} = \Delta_{\mathrm{id},\sigma(a)a(\sigma,\sigma^{-1})},$$

hence substitude $a = \sigma^{-1}\left(a\left(\sigma,\sigma^{-1}\right)^{-1} a(\mathrm{id},\mathrm{id})^{-1}\right)$, the right hand side is again $\Delta_{\mathrm{id},a(\mathrm{id},\mathrm{id})^{-1}}$ which is precisely $1 \in \mathfrak{C}_a$. □

Lemma 4.4.15. For any $c \in K$, we have

$$\Delta_{\sigma,1}\,\iota_a(c) = \iota_a(\sigma \cdot c)\Delta_{\sigma,1} = \Delta_{\sigma,\sigma\cdot c}$$

and consequently,

$$\Delta_{\sigma,1}\,\iota_a(c)\,\Delta_{\sigma,1}^{-1} = \iota_a(\sigma \cdot c).$$

Proof. We calculate

$$\begin{aligned}\Delta_{\sigma,1}\,\iota_a(c) &= \Delta_{\sigma,1}\,\Delta_{\mathrm{id},ca(\mathrm{id},\mathrm{id})^{-1}}\\ &= \Delta_{\sigma,\sigma(ca(\mathrm{id},\mathrm{id})^{-1})a(\sigma,1)}\\ &= \Delta_{\sigma,\sigma(c)\sigma(a(\mathrm{id},\mathrm{id}))^{-1}\sigma(a(\mathrm{id},\mathrm{id}))}\\ &= \Delta_{\sigma,\sigma(c)}.\end{aligned}$$

□

Lemma 4.4.16. We have $\Delta_{\sigma,1}\,\Delta_{\tau,1} = \iota_a(a(\sigma,\tau))\Delta_{\sigma\tau,1} = a(\sigma,\tau)\cdot\Delta_{\sigma\tau,1}$ Consequently we have for any $c, d \in K$,

$$\Delta_{\sigma,c}\Delta_{\tau,d} = (c\sigma(d)a(\sigma,\tau))\cdot\Delta_{\sigma\tau,1}.$$

Proof. The first equality is in construction 4.4.8. For the second equality, by lemma 4.4.15, we have

$$\begin{aligned}\Delta_{\sigma,c}\Delta_{\sigma,d} &= (c\cdot\Delta_{\sigma,1})\,(d\cdot\Delta_{\tau,1})\\ &= \iota_a(c)\,(\Delta_{\sigma,1}\iota_a(d))\,\Delta_{\tau,1}\\ &= \iota_a\Delta_{\sigma,\sigma\cdot d}\Delta_{\tau,1}\\ &= c\cdot\sigma(d)\cdot\Delta_{\sigma,1}\Delta_{\tau,1}\\ &= c\cdot\sigma(d)\cdot a(\sigma,\tau)\cdot\Delta_{\sigma\tau,1}.\end{aligned}$$

□

Lemma 4.4.17. The set $\{\Delta_{\sigma,1}|\sigma\in \mathrm{Gal}(K/F)\}$ forms a K-basis for $\mathfrak{C}_a$.

Proof. Suppose some linear combination $\sum_\sigma \lambda_\sigma\cdot\Delta_{\sigma,1}$ is 0 for some λ_σ's in K. We have, by the equality in construction 4.4.8

$$\sum_{\sigma\in\mathrm{Gal}(K/F)} \lambda_\sigma\cdot\Delta_{\sigma,1} = \sum_{\sigma\in\mathrm{Gal}(K/F)} \Delta_{\sigma,\lambda_\sigma} = 0.$$

Thus, for any $\tau\in\mathrm{Gal}(K/F)$, we have

$$\left(\sum_{\sigma\in\mathrm{Gal}(K/F)} \lambda_\sigma\cdot\Delta_{\sigma,1}\right)(\tau) = 0 = \lambda_\tau,$$

which proves linear independence. The fact that $\{\Delta_{\sigma,1}|\sigma\in\mathrm{Gal}(K/F)\}$ spans $\mathfrak{C}_a$ is easy to see because every $\Delta_{\tau,a} = a\cdot\Delta_{\tau,1}$ is certainly in the span. □

Corollary 4.4.18. When K/F is a finite dimensional Galois extension, the K-dimension of $\mathfrak{C}_a$ is $\dim_F K$ and the F-dimension of $\mathfrak{C}_a$ is $(\dim_F K)^2$.

Now we see that cross product, like a good representation, is a K-module and F-algebra with a K-embedding and correct F-dimension. In the next sections, we prove that $\mathfrak{C}_a$ is in fact a central simple F-algebra.

Central Algebra

We will assume K/F is a finite dimensional Galois extension.

Theorem 4.4.19 (Centrality). $\mathfrak{C}_{\mathfrak{a}}$ is a central F-algebra.

Proof. Let $z \in \mathfrak{C}_{\mathfrak{a}}$ that is in the centre. We want to prove that z is in F. We write z as $\sum_{\sigma} \lambda_{\sigma} \cdot \Delta_{\sigma,1}$. We see that, for any $\tau \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})$, we have

$$z = \sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} \lambda_{\tau^{-1}\sigma\tau} \cdot \Delta_{\tau^{-1}\sigma\tau,1}.$$

Therefore for any $d \in \mathsf{K}$ and $\tau \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})$, by lemma 4.4.16 and lemma 4.4.15, we have

$$\begin{aligned}
z\Delta_{\tau,d} &= \sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} \lambda_{\sigma} \cdot \Delta_{\sigma,1}\Delta_{\tau,d} \\
&= \sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} \lambda_{\sigma} \cdot \sigma(d) \cdot \mathfrak{a}(\sigma,\tau) \cdot \Delta_{\sigma\tau,1} \\
&= \sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} (\lambda_{\sigma}\sigma(d)\mathfrak{a}(\sigma,\tau)) \cdot \Delta_{\sigma\tau,1} \\
\Delta_{\tau,d}\, z &= \sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} \Delta_{\tau,d}\left(\lambda_{\tau^{-1}\sigma\tau} \cdot \Delta_{\tau^{-1}\sigma\tau,1}\right) \\
&= \sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} \Delta_{\tau,d}\iota_{\mathfrak{a}}\left(\lambda_{\tau^{-1}\sigma\tau}\right)\Delta_{\tau^{-1}\sigma\tau,1} \\
&= \sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} d \cdot \Delta_{\tau,1}\iota_{\mathfrak{a}}\left(\lambda_{\tau^{-1}\sigma,\tau}\right)\Delta_{\tau^{-1}\sigma\tau,1} \\
&= \sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} d \cdot \Delta_{\tau,\tau\cdot\lambda_{\tau^{-1}\sigma\tau}}\Delta_{\tau^{-1}\sigma\tau,1} \\
&= \sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} d \cdot \tau\left(\lambda_{\tau^{-1}\sigma\tau}\right) \cdot \Delta_{\tau,1}\Delta_{\tau^{-1}\sigma\tau,1} \\
&= \sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} d \cdot \tau\left(\lambda_{\tau^{-1}\sigma\tau}\right) \cdot \mathfrak{a}\left(\tau,\tau^{-1}\sigma\tau\right) \cdot \Delta_{\sigma\tau,1} \\
&= \sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} \left(d\tau\left(\lambda_{\tau^{-1}\sigma\tau}\right)\mathfrak{a}\left(\tau,\tau^{-1}\sigma\tau\right)\right) \cdot \Delta_{\sigma\tau,1}.
\end{aligned}$$

By lemma 4.4.17, for any $\sigma,\tau \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})$ and $d \in \mathsf{K}$, we have that

$$\lambda_{\sigma}\sigma(d)\mathfrak{a}(\sigma,\tau) = d\tau\left(\lambda_{\tau^{-1}\sigma\tau}\right)\mathfrak{a}\left(\tau,\tau^{-1}\sigma\tau\right). \tag{4.3}$$

In particular, with $d = 1$, we have

$$\lambda_{\sigma}\mathfrak{a}(\sigma,\tau) = \tau\left(\lambda_{\tau^{-1}\sigma\tau}\right)\mathfrak{a}\left(\tau,\tau^{-1}\sigma\tau\right),$$

we substitute back into eq. (4.3) and get

$$\lambda_{\sigma}\sigma(d)\mathfrak{a}(\sigma,\tau) = d\lambda_{\sigma}\mathfrak{a}(\sigma,\tau).$$

With $\tau = \mathsf{id}$, we have

$$\lambda_\sigma \sigma(d) \mathfrak{a}(\sigma, \mathsf{id}) = d\lambda_\sigma \mathfrak{a}(\sigma, \mathsf{id}),$$

Hence for all $d \in K$ with $\lambda_\sigma \neq 0$, we have $\sigma(d) = d$. We immediately deduce that for all $\sigma \neq \mathsf{id}$, $\lambda_\sigma = 0$ by contraposition. Thus $z = \lambda_{\mathsf{id}} \Delta_{\mathsf{id},1} = \Delta_{\mathsf{id},\lambda_{\mathsf{id}}} = \iota_\mathfrak{a}(\lambda_{\mathsf{id}} \mathfrak{a}(\mathsf{id}, \mathsf{id})) = (\lambda_{\mathsf{id}} \mathfrak{a}(\mathsf{id}, \mathsf{id})) \cdot 1$. Consequently, to prove z is in F, it is sufficient to prove that $\lambda_{\mathsf{id}} \mathfrak{a}(\mathsf{id}, \mathsf{id})$ is in F. Since K/F is finite dimensional and Galois, we only need to prove that $\lambda_{\mathsf{id}} \mathfrak{a}(\mathsf{id}, \mathsf{id})$ is fixed by every $\tau \in \mathrm{Gal}(K/F)$.Indeed, with $d = 1$ and $\sigma = \mathsf{id}$ in eq. (4.3), we have

$$\begin{aligned}
\lambda_{\mathsf{id}} \mathfrak{a}(\mathsf{id}, \tau) &= \tau(\lambda_{\mathsf{id}}) \mathfrak{a}(\tau, \mathsf{id}) \\
&= \lambda_{\mathsf{id}} \mathfrak{a}(\mathsf{id}, \mathsf{id}) \\
&= \tau(\lambda_{\mathsf{id}}) \tau(\mathfrak{a}(\mathsf{id}, \mathsf{id})) \\
&= \tau(\lambda_{\mathsf{id}} \mathfrak{a}(\mathsf{id}, \mathsf{id})).
\end{aligned}$$

□

Simple Ring

In this section we assume K/F is a finite dimensional field extension. Let $I \subseteq \mathfrak{C}_\mathfrak{a}$ be a two sided ideal, we aim to show that either $I = \{0\}$ or $I = \mathfrak{C}_\mathfrak{a}$. In this section, we use π to denote the canonical ring homomorphism $\mathfrak{C}_\mathfrak{a} \to {}^{\mathfrak{C}_\mathfrak{a}}/_I$. We restrict π to $\pi|_{\mathrm{im}(\iota_\mathfrak{a})} : \mathrm{im}(\iota_\mathfrak{a}) \to {}^{\mathfrak{C}_\mathfrak{a}}/_I$ and denote the range of $\pi|_{\mathrm{im}(\iota_\mathfrak{a})}$ to be Π.

Construction 4.4.9. The quotient ring ${}^{\mathfrak{C}_\mathfrak{a}}/_I$ is a Π-module defined by $\pi(\iota_\mathfrak{a}(a)) \cdot \pi(y) := \pi(a \cdot y)$. We first check that the Π-action is well-defined:

- Independence of a: Let $a, b \in K$ be such that $\pi(\iota_\mathfrak{a}(a)) = \pi(\iota_\mathfrak{a}(b))$, that is, $\iota_\mathfrak{a}(a - b) \in I$. Since I is a two sided ideal, $a \cdot y - b \cdot y = (a - b) \cdot y = \iota_\mathfrak{a}(a - b)y$ is also in I. This proves $\pi(a \cdot y) = \pi(b \cdot y)$.
- Independence of y: Let $y_1, y_2 \in \mathfrak{C}_\mathfrak{a}$ be such that $y_1 - y_2 \in I$, then for any $a \in K$, $a \cdot y_1 - a \cdot y_2 = \iota_\mathfrak{a}(a)(y_1 - y_2)$ is in I because I is a two sided ideal. This proves $\pi(\iota_\mathfrak{a}(a)) \cdot \pi(y_1) = \pi(\iota_\mathfrak{a}(a)) \cdot \pi(y_2)$.

Then we check the axioms of module:

- Let $y \in \mathfrak{C}_\mathfrak{a}$, we check that $1 \cdot \pi(y) = \pi(y)$ and $0 \cdot \pi(y) = 0$. This is because $\Pi \ni 1 = \pi(\iota_\mathfrak{a}(1))$ and $\Pi \ni 0 = \pi(\iota_\mathfrak{a}(0))$. Let $a \in K$, $\pi(\iota_\mathfrak{a}(a)) \cdot 0 = 0$ because $0 \in {}^{\mathfrak{C}_\mathfrak{a}}/_I$ is equal to $\pi(0)$.
- Let $a, b \in K$ and $x, y \in \mathfrak{C}_\mathfrak{a}$, we check $(\pi(\iota_\mathfrak{a}(a)) + \pi(\iota_\mathfrak{a}(b))) \cdot \pi(x) = \pi(\iota_\mathfrak{a}(a)) \cdot \pi(x) + \pi(\iota_\mathfrak{a}(b)) \cdot \pi(x)$ and $\pi(\iota_\mathfrak{a}(a)) \cdot (\pi(x) + \pi(y)) = \pi(\iota_\mathfrak{a}(a)) \cdot \pi(x) + \pi(\iota_\mathfrak{a}(a)) \cdot \pi(y)$. These are true because π preserves addition. Similarly $\pi(\iota_\mathfrak{a}(a)) \cdot \pi(\iota_\mathfrak{a}(b)) \cdot \pi(x) = \pi(\iota_\mathfrak{a}(ab)) \cdot \pi(x)$ because π preserves multiplication as well.

Hence ${}^{\mathfrak{C}_\mathfrak{a}}/_I$ is also a K-module by pulling back the Π-module structure along $K \to \Pi$ given by $a \mapsto \pi(\iota_\mathfrak{a}(a))$. Note that π is a K-linear map between $\mathfrak{C}_\mathfrak{a}$ and ${}^{\mathfrak{C}_\mathfrak{a}}/_I$ by this construction.

Lemma 4.4.20. If $I \neq \mathfrak{C}_\mathfrak{a}$, the set $\{\pi(\Delta_{\sigma,1}) \mid \sigma \in \mathrm{Gal}(K/F)\}$ forms a K-basis for ${}^{\mathfrak{C}_\mathfrak{a}}/_I$.

Proof. It is easy to see that the set spans ${}^{\mathfrak{C}_a}/_{I}$ because $\{\Delta_{\sigma,1}|\sigma \in \mathrm{Gal}(K/F)\}$ spans $\mathfrak{C}_a$ (lemma 4.4.17). For linear-independence, the idea is the same as in the proof of theorem 4.3.10. We repeat the argument here.

Suppose that $\{\pi(\Delta_{sigma,1})|\sigma \in \mathrm{Gal}(K/F)\}$ is linearly dependent. Let $J \subseteq \mathrm{Gal}(K/F)$ be such that $\{\pi(\Delta_{\sigma,1})|\sigma \in J\}$ is the maximally linearly independent set. Let σ be an arbitrary automorphism that is not in J. Therefore, we have $\pi(\Delta_{\sigma,1}) \in \langle \pi(\Delta_{\tau,1})|\tau \in J\rangle$. Hence we have, by construction 4.4.9 and construction 4.4.8

$$\pi(\Delta_{\sigma,1}) = \sum_{\tau\in J'} \lambda_\tau \cdot \pi(\Delta_{\tau,1}) = \sum_{\tau\in J'} \pi(\iota_a(\lambda_\tau))\,\pi(\Delta_{\tau,1}) = \sum_{\tau\in J'} \pi(\iota_a(\lambda_\tau)\,\Delta_{\tau,1}) = \sum_{\tau\in J'} \pi(\lambda_\tau \cdot \Delta_{\tau,1}).$$

for some non-zero $\lambda_\tau \in K$ and some $J' \subseteq J$. Hence, for any $c \in K$, we have

$$\begin{aligned}
\pi(\iota_a(\sigma\cdot c))\,\pi(\Delta_{\sigma,1}) &= \pi(\Delta_{\sigma,1})\,\pi(\iota_a(c)) && \text{by lemma 4.4.15}\\
&= \sum_{\tau\in J} \pi(\iota_a(\lambda_\tau))\,\pi(\Delta_{\tau,1})\,\pi(\iota_a(c))\\
&= \sum_{\tau\in J} \pi(\iota_a(\lambda_\tau)\,\Delta_{\tau,1}\iota_a c)\\
&= \sum_{\tau\in J} \pi(\iota_a(\lambda_\tau)\,\iota_a(\tau\cdot c)\Delta_{\tau,1}) && \text{by lemma 4.4.15 again}\\
&= \sum_{\tau\in J} \pi(\iota_a(\lambda_\tau\tau(c)))\,\pi(\Delta_{\tau,1})\\
&= \sum_{\tau\in J} (\lambda_\tau\tau(c))\cdot\pi(\Delta_{\tau,1})\\
\pi(\iota_a(\sigma\cdot c))\,\pi(\Delta_{\sigma,1}) &= \sum_{\tau\in J} \pi(\iota_a(\sigma\cdot c))\,\pi(\iota_a(\lambda_\tau))\,\pi(\Delta_{\tau,1})\\
&= \sum_{\tau\in J} \pi(\iota_a(\sigma(c)\lambda_\tau))\,\pi(\Delta_{\tau,1})\\
&= \sum_{\tau\in J} (\sigma(c)\lambda_\tau)\cdot\pi(\Delta_{\tau,1}).
\end{aligned}$$

Since, $\{\pi(\Delta_{\tau,1})|\tau \in J\}$ is linearly independent, for all $c \in K$ and $\tau \in J$, we have that $\lambda_\tau\tau(c) = \sigma(c)\lambda_\tau$. Note that $J' \neq \emptyset$, otherwise, $\pi(\Delta_{\sigma,1}) = 0$ implying that $\Delta_{\sigma,1} \in I$ which by lemma 4.4.14 is invertible but I does not equal to $\mathfrak{C}_a$. Hence for each $\tau \in J'$, we have that for all $c \in K$, since λ_τ is not zero, $\sigma(c) = \tau(c)$, i.e. $\sigma = \tau$. Therefore, σ is in $J' \subseteq J$ after all. □

Corollary 4.4.21. If $I \neq \mathfrak{C}_a$, the quotient ring ${}^{\mathfrak{C}_a}/_{I}$ is isomorphic to $\mathfrak{C}_a$ as K-modules. In particular π is a K-linear isomorphism between $\mathfrak{C}_a$ and the quotient ring ${}^{\mathfrak{C}_a}/_{I}$.

Proof. Indeed, by lemma 4.4.17, $\{\Delta_{\sigma,1}|\sigma \in \mathrm{Gal}(K/F)\}$ is a K-basis for $\mathfrak{C}_a$; and by lemma 4.4.20, $\{\pi(\Delta_{\sigma,1})|\sigma \in \mathrm{Gal}(K/F)\}$ is a K-basis for ${}^{\mathfrak{C}_a}/_{I}$. The two sets obviously biject. Hence we can define a K-linear isomorphism by $\Delta_{\sigma,1} \mapsto \pi(\Delta_{\sigma,1})$. This isomorphism is equal to π everywhere. □

Corollary 4.4.22 (Simple Ring). $\mathfrak{C}_a$ is a simple ring.

Proof. For any two-sided-ideal I that is not equal to $\mathfrak{C}_a$, by corollary 4.4.21, $\pi : \mathsf{cross}_a \to {}^{\mathfrak{C}_a}/_{I}$ is a K-linear isomorphism, therefore I is equal to 0. □

Theorem 4.4.23. Let K/F be a finite dimensional and Galois field extension and $\mathfrak{a}$ be a 2-cocycle in $\mathcal{B}^2(\mathrm{Gal}(K/F), K^\star)$, $\mathfrak{C}_\mathfrak{a}$ is a finite dimensional central simple F-algebra.

Proof. Theorem 4.4.19, lemma 4.4.17 and corollary 4.4.22. □

4.4.3 From $H^2(\mathrm{Gal}(K/F), K^\star)$ to $\mathrm{Br}(K/F)$

For every 2-cocycle $\mathfrak{a}$, we have defined the cross product $\mathfrak{C}_\mathfrak{a}$ and proved that it is indeed a finite dimensional central simple F-algebra in theorem 4.4.23; that is we have a function from $\mathcal{B}^2(\mathrm{Gal}(K/F), K^\star)$ to $\mathbb{CSA}_F$. If we want a function from $H^2(\mathrm{Gal}(K/F), K^\star)$ to $\mathrm{Br}(K/F)$, we need to show that if $\mathfrak{a}$ and $\mathfrak{b}$ are cohomologous, $\mathfrak{C}_\mathfrak{a}$ and $\mathfrak{C}_\mathfrak{b}$ are Brauer equivalent. We state it as a theorem:

Theorem 4.4.24. If K/F is a finite dimensional and Galois field extension, the function $\mathfrak{C}$: $H^2(\mathrm{Gal}(K/F), K^\star) \to \mathrm{Br}(K/F)$ defined by

$$\mathfrak{a} \mapsto [\mathfrak{C}_\mathfrak{a}]_{\sim_{\mathrm{Br}}}$$

is well-defined.

Proof. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two cohomologous 2-cocycles. By definition 4.4.1, for some $\mathfrak{c} : \mathrm{Gal}(K/F) \to K^\star$, for all $\sigma, \tau \in \mathrm{Gal}(K/F)$, we have

$$\frac{\sigma(\mathfrak{c}(\tau))}{\mathfrak{c}(\sigma\tau)}\mathfrak{c}(\sigma) = \frac{\mathfrak{a}(\sigma,\tau)}{\mathfrak{b}(\sigma,\tau)}. \tag{4.4}$$

Let us denote A to be the K-basis $\{\Delta^{\mathfrak{a}}_{\sigma,1} | \sigma \in \mathrm{Gal}(K/F)\}$ for $\mathfrak{C}_\mathfrak{a}$ and B to be the K-basis $\{\mathfrak{c}(\sigma) \cdot \Delta^{\mathfrak{b}}_{\sigma,1} | \sigma \in \mathrm{Gal}(K/F)\}$ for $\mathfrak{C}_\mathfrak{b}$. We immediately have a K-linear isomorphism $\phi : \mathfrak{C}_\mathfrak{a} \cong \mathfrak{C}_\mathfrak{b}$ by mapping A to B. Since the K-action on $\mathfrak{C}_\mathfrak{a}$ and $\mathfrak{C}_\mathfrak{b}$ agrees with the F-action on them (construction 4.4.8), ϕ is also an F-linear isomorphism. We check that $\phi(1) = 1$ and $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in \mathfrak{C}_\mathfrak{a}$:

1. preservation of one: with $\sigma = \tau = \mathrm{id}$ in eq. (4.4), we have $\mathfrak{c}(\mathrm{id}) = \mathfrak{a}(\mathrm{id},\mathrm{id})\mathfrak{b}(\mathrm{id},\mathrm{id})^{-1}$, thus

$$\begin{aligned}
\phi(1) &= \phi\left(\Delta^{\mathfrak{a}}_{\mathrm{id},\mathfrak{a}(\mathrm{id},\mathrm{id})^{-1}}\right) \\
&= \phi\left(\mathfrak{a}(\mathrm{id},\mathrm{id})^{-1} \cdot \Delta^{\mathfrak{a}}_{\mathrm{id},1}\right) \\
&= \mathfrak{a}(\mathrm{id},\mathrm{id})^{-1} \cdot \mathfrak{c}(\mathrm{id}) \cdot \Delta^{\mathfrak{b}}_{\mathrm{id},1} \\
&= \mathfrak{a}(\mathrm{id},\mathrm{id})^{-1} \cdot \mathfrak{c}(\mathrm{id}) \cdot \mathfrak{b}(\mathrm{id},\mathrm{id}) \cdot \mathfrak{b}(\mathrm{id},\mathrm{id})^{-1} \cdot \Delta^{\mathfrak{b}}_{\mathrm{id},1} \\
&= \left(\mathfrak{a}(\mathrm{id},\mathrm{id})^{-1}\mathfrak{c}(\mathrm{id})\mathfrak{b}(\mathrm{id},\mathrm{id})\right) \cdot \left(\mathfrak{b}(\mathrm{id},\mathrm{id})^{-1} \cdot \Delta_{\mathrm{id},1}\right) \\
&= \left(\mathfrak{a}(\mathrm{id},\mathrm{id})^{-1}\mathfrak{a}(\mathrm{id},\mathrm{id})\right) \cdot \Delta_{\mathrm{id},\mathfrak{b}(\mathrm{id},\mathrm{id})^{-1}} \\
&= \Delta_{\mathrm{id},\mathfrak{b}(\mathrm{id},\mathrm{id})^{-1}}.
\end{aligned}$$

2. preservation of multiplication: let $\sigma, \tau \in \mathrm{Gal}(K/F)$ and $a, b \in K$, we need to prove that $\phi\left(\Delta^{\mathfrak{a}}_{\sigma,a}\Delta^{\mathfrak{a}}_{\tau,b}\right) = \phi\left(\Delta^{\mathfrak{a}}_{\sigma,a}\right)\phi\left(\Delta^{\mathfrak{b}}_{\tau,b}\right)$. From eq. (4.4), we see that

$$\sigma(\mathfrak{c}(\tau))\mathfrak{c}(\sigma)\mathfrak{b}(\sigma,\tau) = \mathfrak{c}(\sigma\tau)\mathfrak{a}(\sigma,\tau).$$

Hence, by lemma 4.4.16 and lemma 4.4.15, we have

$$
\begin{aligned}
\phi\left(\Delta^{\mathfrak{a}}_{\sigma,a}\Delta^{\mathfrak{a}}_{\tau,b}\right) &= \phi\left(\Delta^{\mathfrak{a}}_{\sigma\tau,a\sigma(b)\mathfrak{a}(\sigma,\tau)}\right) \\
&= \phi\left(a\sigma(b)\mathfrak{a}(\sigma,\tau)\cdot\Delta^{\mathfrak{a}}_{\sigma\tau,1}\right) \\
&= a\sigma(b)\mathfrak{a}(\sigma,\tau)\cdot\phi\left(\Delta^{\mathfrak{a}}_{\sigma\tau,1}\right) \\
&= a\sigma(b)\mathfrak{a}(\sigma,\tau)\mathfrak{c}(\sigma\tau)\cdot\Delta^{\mathfrak{b}}_{\sigma\tau,1}. \\
&= a\sigma(b)\sigma(\mathfrak{c}(\tau))\mathfrak{c}(\sigma)\mathfrak{b}(\sigma,\tau)\cdot\Delta^{\mathfrak{b}}_{\sigma\tau,1} \\
&= \mathfrak{c}(\sigma)\sigma(\mathfrak{c}(\tau))\cdot\Delta^{\mathfrak{b}}_{\sigma\tau,a\sigma(b)\mathfrak{b}(\sigma\tau)} \\
&= \mathfrak{c}(\sigma)\sigma(\mathfrak{c}(\tau))\cdot\Delta^{\mathfrak{b}}_{\sigma,a}\Delta^{\mathfrak{b}}_{\tau,b} \\
\phi\left(\Delta^{\mathfrak{a}}_{\sigma,a}\right)\phi\left(\Delta^{\mathfrak{a}}_{\tau,b}\right) &= \phi\left(a\cdot\Delta^{\mathfrak{a}}_{\sigma,1}\right)\phi\left(b\cdot\Delta^{\mathfrak{a}}_{\tau,1}\right) \\
&= \left(a\cdot\phi\left(\Delta^{\mathfrak{a}}_{\sigma,1}\right)\right)\left(b\cdot\phi\left(\Delta^{\mathfrak{a}}_{\tau,1}\right)\right) \\
&= \left(a\mathfrak{c}(\sigma)\cdot\Delta^{\mathfrak{b}}_{\sigma,1}\right)\left(b\mathfrak{c}(\tau)\cdot\Delta^{\mathfrak{b}}_{\tau,1}\right) \\
&= a\mathfrak{c}(\sigma)\cdot\left(\Delta^{\mathfrak{b}}_{\sigma,1}\iota_{\mathfrak{b}}(b\mathfrak{c}(\tau))\right)\Delta^{\mathfrak{b}}_{\tau,1} \\
&= a\mathfrak{c}(\sigma)\cdot\Delta^{\mathfrak{b}}_{\sigma,\sigma(b\mathfrak{c}(\tau))}\Delta^{\mathfrak{b}}_{\tau,1} \\
&= a\mathfrak{c}(\sigma)\sigma(b)\sigma(\mathfrak{c}(\tau))\cdot\Delta^{\mathfrak{b}}_{\sigma,1}\Delta^{\mathfrak{b}}_{\tau,1} \\
&= a\mathfrak{c}(\sigma)\sigma(b)\sigma(\mathfrak{c}(\tau))\mathfrak{b}(\sigma,\tau)\cdot\Delta^{\mathfrak{b}}_{\sigma\tau,1} \\
&= \mathfrak{c}(\sigma)\sigma(\mathfrak{c}(\tau))\cdot\Delta^{\mathfrak{b}}_{\sigma\tau,a\sigma(b)\mathfrak{b}(\sigma,\tau)} \\
&= \mathfrak{c}(\sigma)\sigma(\mathfrak{c}(\tau))\cdot\Delta^{\mathfrak{b}}_{\sigma,a}\Delta^{\mathfrak{b}}_{\tau,b}.
\end{aligned}
$$

Hence ϕ is actually an F-algebra isomorphism between $\mathfrak{C}_{\mathfrak{a}}$ and $\mathfrak{C}_{\mathfrak{b}}$ and isomorphic central simple F-algebras are certainly Brauer equivalent. □

4.4.4 $H^2 \circ \mathfrak{C}$ and $\mathfrak{C} \circ H^2$

For a finite dimensional Galois extension of field K/F, we have constructed two functions H^2 and $\mathfrak{C}$ between the second cohomology group $H^2(\mathrm{Gal}(K/F), K^\star)$ and the relative Brauer group $\mathrm{Br}(K/F)$. In this section, we prove that they are mutual inverse to one another,

Lemma 4.4.25. The composition of $\mathfrak{C}$ and H^2 is the identity:

$$
\underbrace{H^2\left(\mathrm{Gal}(K/F), K^\star\right) \xrightarrow{\ \mathfrak{C}\ } \mathrm{Br}(K/F) \xrightarrow{\ H^2\ } H^2\left(\mathrm{Gal}(K/F), K^\star\right)}_{\mathsf{id}}.
$$

Proof. Let $\mathfrak{a}$ be any 2-cocycle, by lemma 4.4.15, we notice that $x : \sigma \mapsto \Delta_{\sigma,1}$ is a conjugation sequence for $\mathfrak{C}_{\mathfrak{a}}$. Hence by construction 4.4.3, ?? and theorem 4.4.24, we evaluate the composition at $\mathfrak{a}$ as:

$$
[\mathfrak{a}] \longmapsto [\mathfrak{C}_{\mathfrak{a}}]_{\sim\mathrm{Br}} \longmapsto \left[(\sigma,\tau) \mapsto \mathrm{comp}^{x}_{\Delta_{\sigma,1},\Delta_{\tau,1},\Delta_{\sigma\tau,1}}\right].
$$

That is, we need to show that $\mathfrak{a}$ and $(\sigma,\tau) \mapsto \mathrm{comp}_{\Delta_{\sigma,1},\Delta_{\tau,1},\Delta_{\sigma\tau,1}}$ are 2-cohomologous. In fact, they are equal. By construction 4.4.2, we have that $\iota_{\mathfrak{C}_{\mathfrak{a}}}\left(\mathrm{comp}^{x}_{\Delta_{\sigma,1},\Delta_{\tau,1},\Delta_{\sigma\tau,1}}\right) = \Delta_{\sigma,1}\Delta_{\tau,1}\Delta^{-1}_{\sigma\tau,1} = \mathfrak{a}(\sigma,\tau)\cdot\Delta_{\sigma\tau,1}\Delta^{-1}_{\sigma\tau,1} = \mathfrak{a}(\sigma,\tau)\cdot 1 = \Delta_{\mathsf{id},\mathfrak{a}(\sigma,\tau)}$ which is precisely $\iota_{\mathfrak{C}_{\mathfrak{a}}}(\mathfrak{a}(\sigma,\tau))$. □

Lemma 4.4.26. The composition of H^2 and $\mathfrak{C}$ is the identity:

$$\mathrm{Br}(K/F) \xrightarrow{H^2} H^2(\mathrm{Gal}(K/F), K^\star) \xrightarrow{\mathfrak{C}} \mathrm{Br}(K/F) \quad (\text{composition} = \mathsf{id}).$$

Proof. Let $X \in \mathrm{Br}(K/F)$, A be an arbitrary good representation of X and x be an arbitrary A-conjugation sequence which exists by corollary 4.3.4 and construction 4.3.4. By definition 4.3.1, $X = [A]_{\sim_{\mathrm{Br}}}$. Hence by ?? and theorem 4.4.24, we evaluate the composition at X as:

$$[A]_{\sim_{\mathrm{Br}}} \longmapsto \left[\mathcal{B}^2_x\right] \longmapsto \left[\mathfrak{C}_{\mathcal{B}^2_x}\right] .$$

Hence we need to prove that A and $\mathfrak{C}_{\mathcal{B}^2_x}$ are Brauer equivalent. We will show that they are isomorphic as F-algebras. since $\{x_\sigma | \sigma \in \mathrm{Gal}(K/F)\}$ is a K-basis for A and $\{\Delta_{\sigma,1} | \sigma \in \mathrm{Gal}(K/F)\}$ is a K-basis for $\mathfrak{C}_{\mathcal{B}^2_x}$, they are certainly isomorphic as K-modules. Let $\phi : \mathfrak{C}_{\mathcal{B}^2_x} \cong A$ be the K-linear isomorphism defined by $\Delta_{\sigma,1} \mapsto x_\sigma$, since the K-action on A and the F-action on A are compatible (construction 4.3.2), ϕ is also an F-linear isomorphism. Like in theorem 4.4.24, we check that $\phi(1) = 1$ and $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in A$:

1. preservation of one: by construction 4.4.2, we have

$$\begin{aligned}
\phi(1) &= \phi\left(\Delta_{\mathsf{id},\mathcal{B}^2_x(\mathsf{id},\mathsf{id})^{-1}}\right) \\
&= \mathcal{B}^2_x(\mathsf{id},\mathsf{id})^{-1}\phi\left(\Delta_{\mathsf{id},1}\right) \\
&= \mathcal{B}^2_x(\mathsf{id},\mathsf{id})^{-1}x_{\mathsf{id}} \\
&= \mathrm{comp}^{-1}_{x_{\mathsf{id}},x_{\mathsf{id}},x_{\mathsf{id}}}\, x_{\mathsf{id}} \\
&= \mathrm{comp}_{x_{\mathsf{id}},x_{\mathsf{id}},x_{\mathsf{id}}}\, x_{\mathsf{id}}x_{\mathsf{id}}x_{\mathsf{id}}^{-1} \\
&= x_{\mathsf{id}}x_{\mathsf{id}}^{-1} \\
&= 1.
\end{aligned}$$

2. preservation of multiplication: let $\sigma, \tau \in \mathrm{Gal}(K/F)$ and $c, d \in K$, by construction 4.4.2 and definition 4.3.3, we have

$$\begin{aligned}
\phi\left(\Delta_{\sigma,c}\Delta_{\tau,d}\right) &= \phi\left(\Delta_{\sigma\tau,c\sigma(d)\mathcal{B}^2_x(\sigma,\tau)}\right) \\
&= c\sigma(d)\mathcal{B}^2_x(\sigma,\tau) \cdot \phi\left(\Delta_{\sigma\tau,1}\right) \\
&= c\sigma(d)\mathcal{B}^2_x(\sigma,\tau) \cdot x_{\sigma\tau} \\
&= c\sigma(d)\,\mathrm{comp}_{x_\sigma,x_\tau,x_{\sigma\tau}} \cdot x_{\sigma\tau} \\
&= c\sigma(d) \cdot \iota_A\left(\mathrm{comp}_{x_\sigma,x_\tau,x_{\sigma\tau}}\right) x_{\sigma\tau} \\
&= c\sigma(d) \cdot x_\sigma x_\tau \\
\phi\left(\Delta_{\sigma,c}\right)\phi\left(\Delta_{\tau,d}\right) &= \left(c \cdot \phi\left(\Delta_{\sigma,1}\right)\right)\left(d \cdot \phi\left(\Delta_{\tau,1}\right)\right) \\
&= \left(c \cdot x_\sigma\right)\left(d \cdot x_\tau\right) \\
&= c \cdot x_\sigma \iota_A(d) x_\tau \\
&= c\sigma_d \cdot x_\sigma x_\tau.
\end{aligned}$$

□

Corollary 4.4.27. For a finite dimensional and Galois extension of field K/F, the relative Brauer group K/F bijects to the second cohomology group $H^2(\mathrm{Gal}(K/F), K^\star)$ by the following commutative diagram

$$\begin{array}{ccc} \mathrm{Br}(K/F) & \xrightarrow{\mathrm{H}^2} & \mathrm{H}^2\left(\mathrm{Gal}(K/F), K^\star\right) \\ \Big\| & & \Big\| \\ \mathrm{Br}(K/F) & \xleftarrow[\mathfrak{C}]{} & \mathrm{H}^2\left(\mathrm{Gal}(K/F), K^\star\right) \end{array} .$$

Proof. Exactly lemma 4.4.25 and lemma 4.4.26. □

4.4.5 Group Homomorphism

In previous sections, when K/F is a finite dimensional Galois extension, we have set up a bijection between the relative Brauer group $\mathrm{Br}(K/F)$ and the second cohomology group $\mathrm{H}^2\left(\mathrm{Gal}(K/F), K^\star\right)$. But both functions H^2 and $\mathfrak{C}$ are only set-theoretical function. In this section, we aim to upgrade them to group homomorphisms. Technically, we only need to prove either one of them preserves multiplication; we provide a proof that H^2 preserves one anyway because we found the proof to be entertaining.

$\mathfrak{C}_1 = 1$ and $\mathrm{H}^2(1) = 1$

Theorem 4.4.28. The function $\mathfrak{C} : \mathrm{H}^2\left(\mathrm{Gal}(K/F), K^\star\right) \to \mathrm{Br}(K/F)$ preserves one, that is $\mathfrak{C}$

Proof. Since $\{\Delta_{\sigma,1} | \sigma \in \mathrm{Gal}(K/F)\}$ is a K-basis for $\mathfrak{C}_1$ where $1 \in \mathcal{B}^2\left(\mathrm{Gal}(K/F), K^\star\right)$ is the constant function 1 (lemma 4.4.17), we construct a K-linear map $\phi : \mathfrak{C}_1 \to \mathrm{End}_F K$ by $\Delta_{\sigma,1} \mapsto \sigma$; note that ϕ is F-linear as well. In fact, ϕ is also an F-algebra homomorphism:

1. $\phi(1) = 1$: indeed $\phi\left(\Delta_{\mathrm{id},1}\right) = \mathrm{id}$.
2. $\phi(xy) = \phi(x)\phi(y)$: indeed, let $\sigma, \tau \in \mathrm{Gal}(K/F)$ and $c, d \in K$, we need to check that $\phi\left(\Delta_{\sigma,c}\Delta_{\tau,d}\right) = \phi\left(\Delta_{\sigma,c}\right)\phi\left(\Delta_{\tau,d}\right)$. The left hand side is equal to

$$\phi\left(\Delta_{\sigma\tau, c\sigma(d)}\right) = \phi\left(c\sigma(d) \cdot \Delta_{\sigma\tau,1}\right) = c\sigma(d) \cdot \sigma\tau;$$

   and the right hand side is equal to

$$\phi\left(c \cdot \Delta_{\sigma,1}\right)\phi\left(d \cdot \Delta_{\tau,1}\right) = (c \cdot \sigma)(d \cdot \tau).$$

   For any $x \in K$, applying left hand side to x will result in $c\sigma(d)\sigma(\tau(x))$ while right hand side will result in $c\sigma(d\tau(x))$, hence both sides are equal.

Hence, ϕ is an F-algebra isomorphism by corollary 1.1.8; that is we have $\mathfrak{C}_1 \cong \mathrm{End}_F K \cong \mathrm{Mat}_{\dim_F K}(F)$. We conclude that $\mathfrak{C}_1$ is Brauer equivalent to F and consequently $\mathrm{H}^2(1) = 1$. □

Corollary 4.4.29. The function $\mathrm{H}^2 : \mathrm{Br}(K/F) \to \mathrm{H}^2\left(\mathrm{Gal}(K/F), K^\star\right)$ preserves one, that is $\mathrm{H}^2(1) = 1$.

Proof. Apply $\mathfrak{C}$ then use lemma 4.4.26 and theorem 4.4.28. □

$\mathfrak{C}_{\mathfrak{ab}} \sim_{\mathrm{Br}} \mathfrak{C}_{\mathfrak{a}} \otimes_{\mathsf{F}} \mathfrak{C}_{\mathfrak{b}}$

The argument in this section is more complicated, because, unlike before, the left hand side and the right hand side are not isomorphic as F-algebras — left hand side has F-dimension $(\dim_{\mathsf{F}} \mathsf{K})$ while the right hand side has F-dimension $(\dim_{\mathsf{F}} \mathsf{K})^4$. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two 2-cocycles in $\mathcal{B}^2(\mathrm{Gal}(\mathsf{K}/\mathsf{F}), \mathsf{K}^\star)$, we denote $\mathfrak{c}$ to be the 2-cocycle $\mathfrak{ab}$. Intuitively, $\mathfrak{C}_{\mathfrak{a}} \otimes_{\mathsf{F}} \mathfrak{C}_{\mathfrak{b}}$ is too "big", to address this issue we introduce a quotient module.

Construction 4.4.10 (M). Consider the quotient module

$$\mathsf{M} := {}^{\mathfrak{C}_{\mathfrak{a}} \otimes_{\mathsf{F}} \mathfrak{C}_{\mathfrak{b}}} \big/ {}_{\langle (k \cdot a) \otimes b - a \otimes (k \cdot b) | k \in \mathsf{K}, a \in \mathfrak{C}_{\mathfrak{a}}, b \in \mathfrak{C}_{\mathfrak{b}} \rangle}.$$

For any $a' \in \mathfrak{C}_{\mathfrak{a}}$ and $b' \in \mathfrak{C}_{\mathfrak{b}}$, we can define an F-linear map $\mathsf{M} \to \mathsf{M}$ by descending the F-linear map $\mathfrak{C}_{\mathfrak{a}} \otimes_{\mathsf{F}} \mathfrak{C}_{\mathfrak{b}} \to \mathfrak{C}_{\mathfrak{a}} \otimes \mathfrak{C}_{\mathfrak{b}}$

$$a \otimes b \mapsto aa' \otimes bb';$$

we need to check that for all $k \in \mathsf{K}, a \in \mathfrak{C}_{\mathfrak{a}}, b \in \mathfrak{C}_{\mathfrak{b}}$, the image of $(k \cdot a) \otimes b - a \otimes (k \cdot b)$ is in $\langle (k \cdot a) \otimes b - a \otimes (k \cdot b) | k \in \mathsf{K}, a \in \mathfrak{C}_{\mathfrak{a}}, b \in \mathfrak{C}_{\mathfrak{b}} \rangle$: the image is $(k \cdot aa') \otimes b - a \otimes (k \cdot bb')$ which is in the generating set with $k \in \mathsf{K}, aa' \in \mathfrak{C}_{\mathfrak{a}}$, and $bb' \in \mathfrak{C}_{\mathfrak{b}}$. This map is in fact F-linear in both a' and b', hence we have an F-bilinear map $\mathfrak{C}_{\mathfrak{a}} \otimes \mathfrak{C}_{\mathfrak{b}} \to \mathsf{M} \to \mathsf{M}$. This gives M a $(\mathfrak{C}_{\mathfrak{a}} \otimes_{\mathsf{F}} \mathfrak{C}_{\mathfrak{b}})^{\mathsf{opp}}$-module structure given by

$$(a' \otimes b') \cdot [a \otimes b] = aa' \otimes bb'$$

for any $a, a' \in \mathfrak{C}_{\mathfrak{a}}$ and $b, b' \in \mathfrak{C}_{\mathfrak{b}}$. All of the module axioms in this case follows from F-bilinearity.

For any $c \in \mathfrak{C}_{\mathfrak{c}}$, we can define another F-linear map $\mathsf{M} \to \mathsf{M}$ by descending the F-linear map $\mathfrak{C}_{\mathfrak{a}} \otimes_{\mathsf{F}} \mathfrak{C}_{\mathfrak{b}} \to \mathfrak{C}_{\mathfrak{a}} \otimes \mathfrak{C}_{\mathfrak{b}}$

$$a \otimes b \mapsto \sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} \Delta^{\mathfrak{a}}_{\sigma, c(\sigma)} a \otimes \Delta^{\mathfrak{b}}_{\sigma,1} b;$$

we need check that for all $k \in \mathsf{K}, a \in \mathfrak{C}_{\mathfrak{a}}, b \in \mathfrak{C}_{\mathfrak{b}}$, the image of $(k \cdot a) \otimes b - a \otimes (k \cdot b)$ is in $\langle (k \cdot a) \otimes b - a \otimes (k \cdot b) | k \in \mathsf{K}, a \in \mathfrak{C}_{\mathfrak{a}}, b \in \mathfrak{C}_{\mathfrak{b}} \rangle$: by lemma 4.4.15 the image is

$$\begin{aligned}
&\sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} \Delta^{\mathfrak{a}}_{\sigma, c(\sigma)} (k \cdot a) \otimes \Delta^{\mathfrak{b}}_{\sigma,1} b - \Delta^{\mathfrak{a}}_{\sigma, c(\sigma)} a \otimes \Delta^{\mathfrak{b}}_{\sigma,1} (k \cdot b) \\
= &\sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} \Delta^{\mathfrak{a}}_{\sigma, c(\sigma)} \iota_{\mathfrak{a}}(k) a \otimes \Delta^{\mathfrak{b}}_{\sigma,1} b - \Delta^{\mathfrak{a}}_{\sigma, c(\sigma)} \otimes \Delta^{\mathfrak{b}}_{\sigma,1} \iota_{\mathfrak{b}}(k) b \\
= &\sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} \sigma(k) \cdot \Delta^{\mathfrak{a}}_{\sigma, c(\sigma)} a \otimes \Delta^{\mathfrak{b}}_{\sigma,1} b - \Delta^{\mathfrak{a}}_{\sigma, c(\sigma)} \otimes \sigma(k) \cdot \Delta^{\mathfrak{b}}_{\sigma,1} b,
\end{aligned}$$

which is in $\langle (k \cdot a) \otimes b - a \otimes (k \cdot b) | k \in \mathsf{K}, a \in \mathfrak{C}_{\mathfrak{a}}, b \in \mathfrak{C}_{\mathfrak{b}} \rangle$ because for each $\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})$, the summand is in the generating set with $\sigma(k) \in \mathsf{K}, \Delta^{\mathfrak{a}}_{\sigma, c(\sigma)} a \in \mathfrak{C}_{\mathfrak{a}}$ and $\Delta^{\mathfrak{b}}_{\sigma,1} b \in \mathfrak{C}_{\mathfrak{b}}$. This map is in fact F-linear in c, therefore we have an F-bilinear map $\mathfrak{C}_{\mathfrak{c}} \to \mathsf{M} \to \mathsf{M}$. (In the above calculation "$\otimes$" symbol has low precedence.) This gives M a $\mathfrak{C}_{\mathfrak{c}}$-module structure given by

$$c \cdot [a \otimes b] = \left[\sum_{\sigma \in \mathrm{Gal}(\mathsf{K}/\mathsf{F})} \Delta^{\mathfrak{a}}_{\sigma, c(\sigma)} a \otimes \Delta^{\mathfrak{b}}_{\sigma,1} b \right].$$

In particular, if c is of the form $k \cdot \Delta^{\mathfrak{c}}_{\tau,1}$, then $(k \cdot \Delta^{\mathfrak{c}}_{\tau,1}) \cdot [a \otimes b]$ is equal to $\left[(k \cdot \Delta^{\mathfrak{a}}_{\tau,1})\, a \otimes \Delta^{\mathfrak{b}}_{\tau,1} b \right]$ because $\Delta^{\mathfrak{c}}_{\tau,1}(\sigma) = 0$ for all $\sigma \neq \tau$. Two of the module axioms need more than F-bilinearity:

- $c = 1$: note that $c = 1 = \mathfrak{b}(\mathrm{id}, \mathrm{id})^{-1}\mathfrak{a}(\mathrm{id}, \mathrm{id})^{-1} \cdot \Delta^{\mathfrak{c}}_{\mathrm{id},1}$, hence

$$\begin{aligned} 1 \cdot [a \otimes b] &= [\mathfrak{b}(\mathrm{id}, \mathrm{id})^{-1}\mathfrak{a}(\mathrm{id}, \mathrm{id})^{-1}\Delta^{\mathfrak{a}}_{\mathrm{id},1}\, a \otimes \Delta^{\mathfrak{b}}_{\mathrm{id},1}\, b] \\ &= [\Delta^{\mathfrak{a}}_{\mathrm{id},\mathfrak{a}(\mathrm{id},\mathrm{id})^{-1}}\, a \otimes \Delta^{\mathfrak{b}}_{\mathrm{id},\mathfrak{b}(\mathrm{id},\mathrm{id})^{-1}}\, b] \\ &= [a \otimes b]. \end{aligned}$$

- $c_1 c_2 \cdot [a \otimes b] = c_1 \cdot c_2 \cdot [a \otimes b]$: assume $c_1 = k_1 \cdot \Delta^{\mathfrak{c}}_{\tau_1,1}$ and $c_2 = k_2 \cdot \Delta^{\mathfrak{c}}_{\tau_2,1}$. Then $c_1 c_2 = k_1 \tau_1(k_2) \cdot \Delta^{\mathfrak{c}}_{\tau_1\tau_2,\mathfrak{c}(\tau_1,\tau_2)} = k_1 \tau_1(k_2)\, \mathfrak{a}(\tau_1, \tau_2)\mathfrak{b}(\tau_1, \tau_2) \cdot \Delta^{\mathfrak{c}}_{\tau_1\tau_2,1}$. Therefore, the left hand side is equal to

$$\begin{aligned} &\left[\left(k_1\tau_1(k_2)\mathfrak{a}(\tau_1, \tau_2)\mathfrak{b}(\tau_1, \tau_2) \cdot \Delta^{\mathfrak{a}}_{\tau_1\tau_2,1}\right) a \otimes \Delta^{\mathfrak{b}}_{\tau_1\tau_2,1}\, b\right] \\ =& \left[k_1\tau_1(k_2)\mathfrak{a}(\tau_1, \tau_2) \cdot \Delta^{\mathfrak{a}}_{\tau_1\tau_2,1}\, a \otimes \mathfrak{b}(\tau_1, \tau_2)\Delta^{\mathfrak{b}}_{\tau_1\tau_2,1}\, b\right] \\ =& \left[\Delta^{\mathfrak{a}}_{\tau_1,k_1}\Delta^{\mathfrak{a}}_{\tau_2,k_2}\, a \otimes \Delta^{\mathfrak{b}}_{\tau_1,1}\Delta^{\mathfrak{b}}_{\tau_2,1}\, b\right]; \end{aligned}$$

  and the right hand side is also equal to

$$\begin{aligned} &\left(k_1 \cdot \Delta^{\mathfrak{c}}_{\tau_1,1}\right)\left[k_2 \cdot \Delta^{\mathfrak{a}}_{\tau_2,1}\, a \otimes \Delta^{\mathfrak{b}}_{\tau_2,1}\, b\right] \\ =& \left[\left(k_1 \cdot \Delta^{\mathfrak{a}}_{\tau_1,1}\right)\left(k_2 \cdot \Delta^{\mathfrak{a}}_{\tau_2,1}\right) a \otimes \Delta^{\mathfrak{b}}_{\tau_1,1}\Delta^{\mathfrak{b}}_{\tau_2,1}\, b\right] \\ =& \left[k_1\tau_1(k_2) \cdot \Delta^{\mathfrak{a}}_{\tau_1\tau_2,\mathfrak{a}(\tau_1,\tau_2)}\, a \otimes \Delta^{\mathfrak{b}}_{\tau_1,1}\Delta^{\mathfrak{b}}_{\tau_2,1}\, b\right] \\ =& \left[\left(k_1 \cdot \Delta^{\mathfrak{a}}_{\tau_1,1}\right)\left(k_2 \cdot \Delta^{\mathfrak{a}}_{\tau_2,1}\right) a \otimes \Delta^{\mathfrak{b}}_{\tau_1,1}\Delta^{\mathfrak{b}}_{\tau_2,1}\, b\right]. \end{aligned}$$

Expanding everything out and checking on the basic elements, we see that for any $x \in (\mathfrak{C}_{\mathfrak{a}} \otimes_F \mathfrak{C}_{\mathfrak{b}})^{\mathrm{opp}}$, $y \in \mathfrak{C}_{\mathfrak{c}}$ and $z \in M$, $x \cdot y \cdot z = y \cdot x \cdot z$. In another word, we gave M a $(\mathfrak{C}_{\mathfrak{c}}, \mathfrak{C}_{\mathfrak{a}} \otimes_F \mathfrak{C}_{\mathfrak{b}})$-bimodule structure.

Lemma 4.4.30. M is isomorphic to $\mathfrak{C}_{\mathfrak{a}} \otimes_K \mathfrak{C}_{\mathfrak{b}}$ as F-modules.

Proof. The map $M \to \mathfrak{C}_{\mathfrak{a}} \otimes_K \mathfrak{C}_{\mathfrak{b}}$ is obtained by descending the obvious F-linear map $\mathfrak{C}_{\mathfrak{a}} \otimes_F \mathfrak{C}_{\mathfrak{b}} \to \mathfrak{C}_{\mathfrak{a}} \otimes_K \mathfrak{C}_{\mathfrak{b}}$. By universal property of tensor product, there is an additive group homomorphism $\mathfrak{C}_{\mathfrak{a}} \otimes_K \mathfrak{C}_{\mathfrak{b}} \to M$ given by $a \otimes b \mapsto [a \otimes b]$, this map is in fact F-linear. The two maps are inverse to each other. □

Corollary 4.4.31. The F-dimension of M is equal to $(\dim_F K)^3$, consequently M is a finitely generated $\mathfrak{C}_{\mathfrak{c}}$-module.

Proof. By lemma 4.4.30, the dimension of M is equal to $\dim_F \mathfrak{C}_{\mathfrak{a}} \otimes_K \mathfrak{C}_{\mathfrak{b}} = \dim_K \mathfrak{C}_{\mathfrak{a}} \otimes_K \mathfrak{C}_{\mathfrak{b}} \dim_F K$. By lemma 4.4.17, $\dim_K \mathfrak{C}_{\mathfrak{a}} = \dim_K \mathfrak{C}_{\mathfrak{b}} = \dim_F K$. □

Construction 4.4.11. By lemma 2.2.2, there exists some simple $\mathfrak{C}_{\mathfrak{c}}$-module S such that $\mathfrak{C}_{\mathfrak{c}}$ is isomorphic to $\bigoplus_{i \in J} S$ as $\mathfrak{C}_{\mathfrak{c}}$-module for some indexing set J. If we give S the F-module structure by pulling back the $\mathfrak{C}_{\mathfrak{c}}$-module structure, by restricting scalars $\mathfrak{C}_{\mathfrak{c}}$ is isomorphic to $\bigoplus_{i \in J} S$ as F-module as well. Since $\mathfrak{C}_{\mathfrak{c}}$ is a finite dimensional F-vector space, J must be finite as well. Note that S must be a finite dimensional F-vector space, because S is finitely generated as $\mathfrak{C}_{\mathfrak{c}}$-module and $\mathfrak{C}_{\mathfrak{c}}$ has finite F-dimension. The indexing set J must be nonempty, otherwise $\mathfrak{C}_{\mathfrak{c}}$ being isomorphic to $\bigoplus_{\emptyset} S$ is a trivial ring; but simple rings are non-trivial. Since J is finite, direct sum over J and direct product over J agree. Recall construction 3.1.1 and construction 3.1.2, for all non-zero $m \in \mathbb{N}$, we have

$$\mathrm{End}_{\mathfrak{C}_{\mathfrak{c}}}(S^m) \cong \mathrm{Mat}_m(\mathrm{End}_{\mathfrak{C}_{\mathfrak{c}}} S)$$

as F-algebras, hence

$$\mathfrak{C}_{\mathfrak{c}}^{\mathsf{opp}} \cong \operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} \mathfrak{C}_{\mathfrak{c}} \cong \operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} S^{|J|} \cong \operatorname{Mat}_{|J|}\left(\operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} S\right)$$

as F-algebras. Finally

$$\mathfrak{C}_{\mathfrak{c}} \cong \operatorname{Mat}_{|J|}\left(\operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}}(S)^{\mathsf{opp}}\right)$$

as F-algebras.

Corollary 4.4.32.

$$(\dim_F K)^2 = |J|^2 \dim_F \operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} S.$$

Proof. They are both equal to $\dim_F \mathfrak{C}_{\mathfrak{c}}$ by construction 4.4.11. □

Corollary 4.4.33.

$$|J| \dim_F S = (\dim_F K)^2$$

Proof. They are all equal to $\dim_F \mathfrak{C}_{\mathfrak{c}} = \dim_F S^{|J|}$ by construction 4.4.11. □

Lemma 4.4.34. There exists a $\mathfrak{C}_{\mathfrak{c}}$-linear isomorphism between M and $S^{|J|\dim_F K}$.

Proof. By lemma 2.2.4, we only need to show that $\dim_F M = \dim_F S^{|J|\dim_F K}$. We already have $\dim_F M = (\dim_F K)^3$ by corollary 4.4.31. We also have $\dim_F S^{|J|\dim_F K} = |J| \dim_F K \dim_F S = \dim_F K\,(|J| \dim_F S) = \dim_F K\,(\dim_F K)^2$ by corollary 4.4.33. □

Corollary 4.4.35. As F-vector spaces, $M \cong S^{|J|\dim_F K}$.

Proof. Restricting scalars on the $\mathfrak{C}_{\mathfrak{c}}$-linear isomorphism in lemma 4.4.34 □

Corollary 4.4.36. As F-algebras, $\operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} M \cong \operatorname{Mat}_{|J|\dim_F K}(\operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} S)$.

Proof. From corollary 4.4.35, we have $\operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} M \cong \operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}}\left(S^{|J|\dim_F K}\right)$. By construction 3.1.2, they are isomorphic to $\operatorname{Mat}_{|J|\dim_F K}(\operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} S)$. □

Corollary 4.4.37.

$$\dim_F \operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} M = (\dim_F K)^4.$$

Proof.

$$\begin{aligned}
\dim_F \operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} M &= \dim_F \operatorname{Mat}_{|J|\dim_F K}(\operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} S) \\
&= \dim_F \left(\operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} S \otimes_F \operatorname{Mat}_{|J|\dim_F K}(F)\right) \\
&= |J|^2 (\dim_F K)^2 \dim_F \operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} S \\
&= (\dim_F K)^2 \left(|J|^2 \dim_F \operatorname{End}_{\mathfrak{C}_{\mathfrak{c}}} S\right) \\
&= (\dim_F K)^2 (\dim_F K)^2,
\end{aligned}$$

where the last equality is by corollary 4.4.32. □

Theorem 4.4.38. The cross product $\mathfrak{C}_{\mathfrak{c}}$ and the tensor product $\mathfrak{C}_{\mathfrak{a}} \otimes_F \mathfrak{C}_{\mathfrak{b}}$ are Brauer equivalent.

Proof. We define an F-algebra homomorphism $\phi : (\mathfrak{C}_\mathfrak{a} \otimes_\mathsf{F} \mathfrak{C}_\mathfrak{b})^{\mathsf{opp}} \to \mathrm{End}_{\mathfrak{C}_\mathfrak{c}} M$ by $x \mapsto (x \cdot \bullet)$. By corollary 4.4.37, both sides has F-dimension $(\dim_\mathsf{F} \mathsf{K})^4$, therefore, ϕ is an F-algebra isomorphism by corollary 1.1.8. Hence we have another F-algebra isomorphism by composing the isomorphism in corollary 4.4.36:

$$\phi^{\mathsf{opp}} : \mathfrak{C}_\mathfrak{a} \otimes_\mathsf{F} \mathfrak{C}_\mathfrak{b} \cong (\mathrm{End}_{\mathfrak{C}_\mathfrak{c}} M)^{\mathsf{opp}} \cong \mathrm{Mat}_{|J| \dim_\mathsf{F} \mathsf{K}} \left((\mathrm{End}_{\mathfrak{C}_\mathfrak{c}} S)^{\mathsf{opp}} \right).$$

In the meantime, by construction 4.4.11, we have $\mathfrak{C}_\mathfrak{c} \cong \mathrm{Mat}_{|J|} \left((\mathrm{End}_{\mathfrak{C}_\mathfrak{c}} S) \, \mathsf{opp} \right)$; hence $\mathrm{Mat}_{\dim_\mathsf{F} \mathsf{K}} (\mathfrak{C}_\mathfrak{c})$ is isomorphic to $\mathfrak{C}_\mathfrak{a} \otimes_\mathsf{F} \mathfrak{C}_\mathfrak{b}$. □

Corollary 4.4.39 (group isomorphism)**.** For a finite dimensional Galois field extension K/F, the relative Brauer group $\mathrm{Br}(\mathsf{K}/\mathsf{F})$ is isomorphic to the second group cohomology $\mathrm{H}^2 \left(\mathrm{Gal}(\mathsf{K}/\mathsf{F}), \mathsf{K}^\star \right)$.

Proof. In corollary 4.4.27, we have seen that H^2 and $\mathfrak{C}$ form a bijection, thus it is sufficient to check either one of them preserves multiplication. The function $\mathfrak{C} : \mathrm{H}^2 \left(\mathrm{Gal}(\mathsf{K}/\mathsf{F}), \mathsf{K}^\star \right)$ preserves multiplication: let $[\mathfrak{a}], [\mathfrak{b}]$ be two elements in $\mathrm{H}^2 \left(\mathrm{Gal}(\mathsf{K}/\mathsf{F}), \mathsf{K}^\star \right)$, by theorem 4.4.38, $\mathfrak{C}(\mathfrak{a}\mathfrak{b})$ is indeed Brauer equivalent to $\mathfrak{C}(\mathfrak{a}) \otimes_\mathsf{F} \mathfrak{C}(\mathfrak{b})$ that is

$$[\mathfrak{C}_\mathfrak{a}]_{\sim_{\mathrm{Br}}} [\mathfrak{C}_\mathfrak{b}]_{\sim_{\mathrm{Br}}} = [\mathfrak{C}_{\mathfrak{a}\mathfrak{b}}].$$

□