III. Brauer Group, 123-165

DOI: 10.3792/euclid/9781429799928-3

from

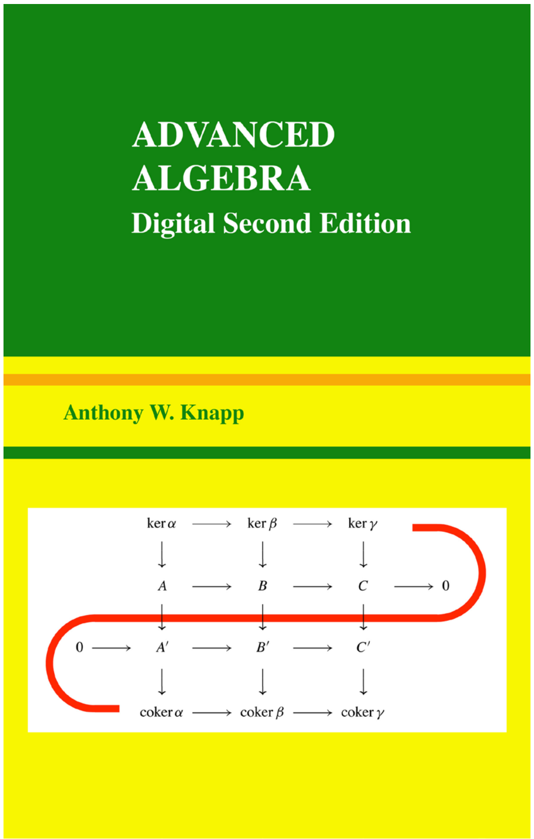
Advanced Algebra

Digital Second Edition

Anthony W. Knapp

Full Book DOI: 10.3792/euclid/9781429799928

ISBN: 978-1-4297-9992-8



ADVANCED
ALGEBRA
Digital Second Edition

Anthony W. Knapp

Anthony W. Knapp
81 Upper Sheep Pasture Road
East Setauket, N.Y. 11733–1729, U.S.A.
Email to: aknapp@math.stonybrook.edu
Homepage: www.math.stonybrook.edu/∼aknapp

Title: Advanced Algebra
Cover: Content of the Snake Lemma; see page 185.

Mathematics Subject Classification (2010): 11–01, 13–01, 14–01, 16–01, 18G99, 55U99, 11R04, 11S15, 12F99, 14A05, 14H05, 12Y05, 14A10, 14Q99.

First Edition, ISBN-13 978-0-8176-4522-9
©2007 Anthony W. Knapp
Published by Birkhäuser Boston

Digital Second Edition, not to be sold, no ISBN
©2016 Anthony W. Knapp
Published by the Author

CHAPTER III

Brauer Group

Abstract. This chapter continues the study of finite-dimensional associative division algebras over a field F, with particular attention to those that are simple and have center F. Section 5 is a self-contained digression on cohomology of groups that is preparation for an application in Section 6 and for a general treatment of homological algebra in Chapter IV.

Section 1 introduces the Brauer group of F and the relative Brauer group of K/F, K being any finite extension field. The Brauer group $\mathcal{B}(F)$ is the abelian group of equivalence classes of finite-dimensional central simple algebras over F under a relation called Brauer equivalence. The inclusion $F \subseteq K$ induces a group homomorphism $\mathcal{B}(F) \to \mathcal{B}(K)$, and the relative Brauer group $\mathcal{B}(K/F)$ is the kernel of this homomorphism. The members of the kernel are those classes such that the tensor product with K of any member of the class is isomorphic to some full matrix algebra $M_n(K)$; such a class always has a representative A with $\dim_F A = (\dim_F K)^2$. One proves that $\mathcal{B}(F)$ is the union of all $\mathcal{B}(K/F)$ as K ranges over all finite Galois extensions of F.

Sections 2–3 establish a group isomorphism $\mathcal{B}(K/F) \cong H^2(\mathrm{Gal}(K/F), K^\times)$ when K is a finite Galois extension of F. With these hypotheses on K and F, Section 2 introduces data called a factor set for each member of $\mathcal{B}(K/F)$. The data depend on some choices, and the effect of making different choices is to multiply the factor set by a "trivial factor set." Passage to factor sets thereby yields a function from $\mathcal{B}(K/F)$ to the cohomology group $H^2(\mathrm{Gal}(K/F), K^\times)$. Section 3 shows how to construct a concrete central simple algebra over F from a factor set, and this construction is used to show that the function from $\mathcal{B}(K/F)$ to $H^2(\mathrm{Gal}(K/F), K^\times)$ constructed in Section 2 is one-one onto. An additional argument shows that this function in fact is a group isomorphism.

Section 4 proves under the same hypotheses that $H^1(\mathrm{Gal}(K/F), K^\times) = 0$, and a corollary makes this result concrete when the Galois group is cyclic. This result and the corollary are known as Hilbert's Theorem 90.

Section 5 is a self-contained digression on the cohomology of groups. If G is a group and $\mathbb{Z}G$ is its integral group ring, a standard resolution of $\mathbb{Z}$ by free $\mathbb{Z}G$ modules is constructed in the category of all unital left $\mathbb{Z}G$ modules. This has the property that if M is an abelian group on which G acts by automorphisms, then the groups $H^n(G, M)$ result from applying the functor $\mathrm{Hom}_{\mathbb{Z}G}(\,\cdot\,, M)$ to the members of this resolution, dropping the term $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M)$, and taking the cohomology of the resulting complex. Section 5 goes on to show that the groups $H^n(G, M)$ arise whenever this construction is applied to any free resolution of $\mathbb{Z}$, not necessarily the standard one. This section serves as a prerequisite for Section 6 and as motivational background for Chapter IV.

Section 6 applies the result of Section 5 in the case that G is finite cyclic, producing a nonstandard free resolution of $\mathbb{Z}$ in this case. From this alternative free resolution, one obtains a rather explicit formula for $H^2(G, M)$ whenever G is finite cyclic. Application to the case that G is the Galois group $\mathrm{Gal}(K/F)$ for a finite Galois extension gives the explicit formula $\mathcal{B}(K/F) \cong F^\times / N_{K/F}(K^\times)$ for the relative Brauer group when the Galois group is cyclic.

1. Definition and Examples, Relative Brauer Group

The "Brauer group" of a field allows one to work with the set of all isomorphism classes of finite-dimensional central division algebras over the field. The core theory in principle reduces the study of all such division algebras to questions in the cohomology theory of groups. The latter theory was introduced in Chapter VII of *Basic Algebra* and will be developed further in the present chapter and the next.

Let F be a field. Theorem 2.4 shows that every finite-dimensional central simple algebra A over F is of the form $A \cong M_n(D)$ for some uniquely determined integer $n \geq 1$ and some finite-dimensional central division algebra D over F that is uniquely determined up to F isomorphism. We can introduce an equivalence relation for finite-dimensional central division algebras over F that exactly mirrors the relation of F isomorphism of the underlying finite-dimensional central division algebras. Specifically if $A \cong M_n(D)$ and $A' \cong M_{n'}(D')$ are two such central simple algebras for the same F such that $D \cong D'$, then we say that A is **Brauer equivalent** to A', and we write $A \sim A'$. It is immediate from the definition that "Brauer equivalent" is an equivalence relation. We shall introduce an abelian-group structure into the set of Brauer equivalence classes, hence into the set of isomorphism classes of central finite-dimensional division algebras over F.

Proposition 10.24 of *Basic Algebra* gives the definition of the tensor product of two F algebras[1] over F, and this operation is associative, up to canonical isomorphism, by Proposition 10.22. It is also commutative, up to canonical isomorphism. In fact, if A and B are given algebras over F, then the canonical vector-space isomorphism $\varphi : A \otimes_F B \to B \otimes_F A$ is given by $\varphi(a \otimes b) = b \otimes a$. If $a_1 \otimes b_1$ and $a_2 \otimes b_2$ are given, then the computation

$$\begin{aligned}\varphi(a_1 \otimes b_1)\varphi(a_2 \otimes b_2) &= (b_1 \otimes a_1)(b_2 \otimes a_2) = b_1 b_2 \otimes a_1 a_2 \\ &= \varphi(a_1 a_2 \otimes b_1 b_2) = \varphi\big((a_1 \otimes b_1)(a_2 \otimes b_2)\big)\end{aligned}$$

shows that φ respects multiplication. Hence tensor product is commutative for algebras, up to canonical isomorphism.

Lemma 3.1. If F is a field, then

(a) $M_n(R) \cong R \otimes_F M_n(F)$ for any algebra R with identity over F,

(b) $M_m(F) \otimes_F M_n(F) \cong M_{(mn)}(F)$.

PROOF. For (a), the F bilinear map $(r, [a_{ij}]) \mapsto [ra_{ij}]$ of $R \times M_n(F)$ into

[1] All algebras in this chapter are understood to be associative.

$M_n(R)$ has a unique linear extension φ to an F linear map of $R \otimes_F M_n(F)$ into $M_n(R)$. The map φ has

$$\begin{aligned}\varphi\big((r \otimes [a_{ij}])(r' \otimes [a'_{ij}])\big) &= \varphi(rr' \otimes [a_{ij}][a'_{ij}]) \\ &= rr'[a_{ij}][a'_{ij}] \\ &= r[a_{ij}]r'[a'_{ij}] \qquad\qquad \text{since each } a_{ij} \text{ is in } F \\ &= \varphi(r \otimes_F [a_{ij}])\varphi(r' \otimes [a'_{ij}]),\end{aligned}$$

and hence φ is an F algebra homomorphism. If $\{r_k\}$ is a vector-space basis of R over F and if $\{E_{ij}\}$ is the usual basis of $M_n(F)$, then $\varphi(r_k \otimes E_{ij}) = r_k E_{ij}$, and it follows that φ carries a vector-space basis onto a vector-space basis. Hence φ is one-one and onto.

For (b), the result of (a) gives $M_m(F) \otimes_F M_n(F) \cong M_n(M_m(F))$, and the algebra on the right is isomorphic to the algebra $M_{(mn)}(F)$ of matrices of size mn by the multiplication-in-blocks isomorphism. □

Proposition 3.2. For the field F, the operation of tensor product on finite-dimensional central simple algebras over F descends to an operation on the set of Brauer equivalence classes of such algebras and makes this set into an abelian group.

PROOF. The tensor product of two finite-dimensional algebras over F is again a finite-dimensional algebra, and Proposition 2.36 shows that the tensor product of two central simple algebras is again central simple. Hence tensor product is well defined as an operation on finite-dimensional central simple algebras over F. Let us see that tensor product is a Brauer class property. Thus suppose that $A \sim A'$ and $B \sim B'$, say with $A = M_m(D)$, $A' \cong M_{m'}(D)$, $B = M_n(E)$, and $B' = M_{n'}(E)$. Since the tensor product of some $M_r(F)$ with an algebra over F, up to isomorphism, does not depend on the order of the two factors and since tensor product is associative up to isomorphism, Lemma 3.1 gives

$$\begin{aligned}A \otimes_F B = M_m(D) \otimes_F M_n(E) &\cong D \otimes_F M_m(F) \otimes_F M_n(F) \otimes_F E \\ &\cong D \otimes_F M_{(mn)}(F) \otimes_F E \cong M_{(mn)}(F) \otimes_F D \otimes_F E \\ &\cong M_{(mn)}(D \otimes_F E).\end{aligned}$$

Similarly $A' \otimes_F B' \cong M_{(m'n')}(D \otimes_F E)$. Thus $A \otimes_F B \sim A' \otimes_F B'$.

We have observed that the tensor product operation on algebras over F is associative and commutative, up to canonical isomorphisms, and hence so is the product operation on Brauer equivalence classes. The class of the 1-dimensional algebra F is the identity, and the class of the opposite algebra A^o is an inverse to the class of A because of the isomorphism $A \otimes_F A^o \cong M_n(F)$ given in Corollary 2.38. □

The abelian group of Brauer equivalence classes of finite-dimensional central simple algebras over F is called the **Brauer group** of F and is denoted by $\mathcal{B}(F)$. We use additive notation for its product operation.

EXAMPLES ALREADY SETTLED IN CHAPTER II.

(1) If F is algebraically closed, then $\mathcal{B}(F) = 0$.

(2) If $F = \mathbb{R}$, then $\mathcal{B}(F) = \mathbb{Z}/2\mathbb{Z}$ by Frobenius's Theorem (Theorem 2.50).

(3) If F is a finite field, then $\mathcal{B}(F) = 0$ by Wedderburn's Theorem about finite division rings (Theorem 2.48).

The group structure for $\mathcal{B}(F)$ given in Proposition 3.2 offers little help by itself in identifying the finite-dimensional division algebras over a particular field. Instead, the usual procedure for understanding $\mathcal{B}(F)$ is to isolate certain special subgroups of $\mathcal{B}(F)$, known as "relative Brauer groups" and denoted by $\mathcal{B}(K/F)$, K being any finite extension of F. Under the assumption that K is a finite Galois extension of F, Theorem 3.14 below says that $\mathcal{B}(K/F)$ is isomorphic to the cohomology group $H^2(G, N)$, where G is the finite group $G = \mathrm{Gal}(K/F)$ and N is the (abelian) multiplicative group $K^\times$ of the field K. This cohomology group is in principle manageable. Corollary 3.9 below says that $\mathcal{B}(F)$ is the union over all finite Galois extensions K/F of $\mathcal{B}(K/F)$, and we therefore obtain a handle on $\mathcal{B}(F)$.

If A is any finite-dimensional central simple algebra over F and if K/F is any field extension, then Proposition 2.36a shows that $A \otimes_F K$ is simple as a ring, and Lemma 2.35b shows that $A \otimes_F K$ has center K. Therefore $A \otimes_F K$ is a central simple algebra over K, and its Brauer equivalence class is a member of $\mathcal{B}(K)$.

Let us see that this map of algebras A into $\mathcal{B}(K)$ depends only on the Brauer equivalence class of A in $\mathcal{B}(F)$. Thus suppose that $A = M_m(D)$ and $A' = M_n(D)$ for some finite-dimensional central division algebra D over F. Lemma 3.1a gives us isomorphisms of F algebras

$$\begin{aligned} A \otimes_F K &\cong M_m(D) \otimes_F K \cong (M_m(F) \otimes_F D) \otimes_F K \\ &\cong M_m(F) \otimes_F (D \otimes_F K) \cong M_m(D \otimes_F K), \end{aligned}$$

and similarly $A' \otimes_F K \cong M_n(D \otimes_F K)$. In each case the left member of the isomorphism is a K algebra, with K contained in the center. Thus we can view each of our isomorphisms as isomorphisms of central simple K algebras. Since $D \otimes_F K$ is a finite-dimensional central simple K algebra, we know that $D \otimes_F K \cong M_r(E)$ for some finite-dimensional central division algebra E over K. Application of Lemma 3.1b allows us to continue the displayed isomorphisms as

$$A \otimes_F K \cong M_m(D \otimes_F K) \cong M_m(M_r(E)) \cong M_{(mr)}(E).$$

Similarly we have $A' \otimes_F K \cong M_{(nr)}(E)$. Thus $A \otimes_F K$ and $A' \otimes_F K$ yield the same member of $\mathcal{B}(K)$, and $(\,\cdot\,) \otimes_F K$ induces a well-defined function from $\mathcal{B}(F)$ into $\mathcal{B}(K)$.

The function from $\mathcal{B}(F)$ into $\mathcal{B}(K)$ is a group homomorphism. In fact, if A and B are finite-dimensional central simple over F, then we have K isomorphisms

$$\begin{aligned}(A \otimes_F K) \otimes_K (B \otimes_F K) &\cong A \otimes_F (K \otimes_K (B \otimes_F K)) \\ &\cong A \otimes_F (B \otimes_F K) \cong (A \otimes_F B) \otimes_F K,\end{aligned}$$

and the map is indeed a group homomorphism.

In addition, the resulting homomorphism satisfies the expected compatibility condition with respect to compositions. In more detail, if we have nested fields $F \subseteq K \subseteq L$, then the L isomorphisms

$$(A \otimes_F K) \otimes_K L \cong A \otimes_F (K \otimes_K L) \cong A \otimes_F L$$

show that the composition of tensoring with K over F, followed by tensoring with L over K, yields the same result as tensoring directly with L over F.

We define the **relative Brauer group** $\mathcal{B}(K/F)$ to be the kernel of the homomorphism of $\mathcal{B}(F)$ into $\mathcal{B}(K)$. The members of the group $\mathcal{B}(K/F)$ are the Brauer equivalence classes of finite-dimensional central simple F algebras A such that $A \otimes_F K$ is F isomorphic to $M_n(K)$ for some n. We say that such algebras are **split** over K, that K **splits** such algebras, and that K is a **splitting field** for these algebras and their Brauer equivalence classes.

Theorem 3.3. Let K/F be a finite extension of fields. Then K is a splitting field for a given member X of $\mathcal{B}(K/F)$ if and only if there exists an algebra A over F in the Brauer equivalence class X containing a subfield K' isomorphic to K such that $\dim_F A = (\dim_F K')^2$.

REMARKS.

(1) The theory of the Brauer group makes repeated use of this result. Corollary 2.47 shows that the subfield K' of A is a maximal commutative subalgebra of A and in particular is a maximal subfield of A.

(2) Observe that the field K is given in the theorem, and hence the integer $n = \dim_F K$ is known. Then A must have dimension n^2. The equality $\dim_F A = n^2$ determines A up to F isomorphism. In fact, Theorem 2.4 shows that $A \cong M_r(D)$ for a central division algebra whose isomorphism class is determined by the class X. Then $n^2 = \dim_F A = r^2 \dim_F D$, and $r^2 = n^2/\dim_F(D)$. So A is indeed determined up to F isomorphism.

(3) In view of the previous remark, any class X in $\mathcal{B}(K/F)$ has a distinguished representative that is unique up to F isomorphism; the distinguished representatives of the members of $\mathcal{B}(K/F)$ for fixed K all have the same dimension.

PROOF. Suppose that A is a central simple algebra in the Brauer equivalence class X containing a subfield K' isomorphic to K such that $\dim_F A = (\dim_F K')^2$. We are to prove that K' splits A. Write n for $\dim_F K'$, so that $\dim_F A = n^2$. Regard A as an n-dimensional K' vector space with K' acting by right multiplication on A. Define an F bilinear mapping $f : A \times K' \to \operatorname{End}_{K'}(A)$ by $f(a, c)(a') = aa'c$; the image $f(a, c)$ is in $\operatorname{End}_{K'}(A)$ because

$$f(a,c)(a'c') = aa'c'c = (aa'c)c' = \big(f(a,c)(a')\big)c'.$$

Extend f without changing its name to an F linear mapping $f : A \otimes_F K' \to \operatorname{End}_{K'}(A)$ such that $f(a \otimes c)(a') = aa'c$. The mapping f is actually K' linear because

$$f((a \otimes c)c')(a') = f(a \otimes cc')(a') = aa'cc' = \big(f(a \otimes c)(a')\big)c'.$$

Also, it respects multiplication, since

$$\begin{aligned} f(a \otimes c)\big(f(a' \otimes c')(a'')\big) &= f(a \otimes c)(a'a''c') = aa'a''c'c = aa'a''cc' \\ &= f(aa' \otimes cc')(a'') = f\big((a \otimes c)(a' \otimes c')\big)(a''). \end{aligned}$$

Thus f is a homomorphism of K' algebras. The domain $A \otimes_F K'$ is central simple over K', as we saw when setting up the homomorphism $\mathcal{B}(F) \to \mathcal{B}(K)$, and therefore f is one-one. Since $A \otimes_F K'$ and $\operatorname{End}_{K'}(A)$ both have K' dimension n^2, f has to be onto. Thus f exhibits $A \otimes_F K'$ as isomorphic to a full matrix ring over K', and K' splits A.

Conversely suppose that K is a splitting field for the members of the class X in $\mathcal{B}(F)$. Let D be a division algebra in the class X. Since $\mathcal{B}(K/F)$ is a group and therefore contains the inverse class D^o, we must have $D^o \otimes_F K \cong M_m(K)$ for the integer m such that $\dim_F D^o = m^2$. Let us rewrite this K isomorphism as $D^o \otimes_F K \cong \operatorname{End}_K(K^m)$. The algebra $\operatorname{End}_F(K^m)$ is central simple over F, and up to an isomorphism, it contains the K algebra $D^o \otimes_F K$ and hence also the F algebra $D^o \otimes_F F \cong D^o$. Let A be the centralizer of D^o in $\operatorname{End}_F(K^m)$. We shall prove that A has the required properties.

The algebra A contains (center D^o) $\otimes_F K$, which is a subfield K' isomorphic to K because D^o is central over F, and A is simple by the Double Centralizer Theorem (Theorem 2.43). The center of A matches the center of the centralizer of A, which is the center of D^o by Theorem 2.43, which in turn is F. Thus A is central simple over F. Yet another application of Theorem 2.43 gives

$$(\dim_F A)(\dim_F D^o) = \dim_F \operatorname{End}_F(K^m) = m^2(\dim_F K)^2. \qquad (*)$$

Since $\dim_F D^o = m^2$, we see that $\dim_F A = (\dim_F K)^2$. Thus the subfield K' of A isomorphic to K has the required dimension.

To see that A is in the Brauer equivalence class X, start from the F bilinear map $A \times (D^o \otimes_F F) \to \operatorname{End}_F(K^m)$ given by $(a, d \otimes 1) \mapsto ad$, and form its F linear extension $\varphi : A \otimes_F (D^o \otimes_F F) \to \operatorname{End}_F(K^m)$. The map φ respects multiplication because the members of A commute with the members of $D^o \otimes_F F$:

$$\begin{aligned}\varphi(a \otimes (d \otimes 1))\big(\varphi(a' \otimes (d' \otimes 1))(v)\big) &= \varphi(a \otimes (d \otimes 1))(a'd'v) = ada'd'v \\ &= aa'dd'v = \varphi(aa' \otimes (dd' \otimes 1))(v).\end{aligned}$$

Since $A \otimes_F (D^o \otimes_F F)$ is simple by Proposition 2.36, φ is one-one. A look at $(*)$ shows that

$$\dim_F(A \otimes_F (D^o \otimes_F F)) = (\dim_F A)(\dim_F D^o) = \dim_F \operatorname{End}_F(K^m)$$

and allows us to conclude that φ is onto. Therefore $A \otimes_F D^o \cong \operatorname{End}_F(K^m)$. Since $\operatorname{End}_F(K^m)$ is Brauer equivalent to F, the Brauer equivalence class of A is the inverse of the class of D^o. Hence the class of A equals the class of D, which is X. □

Corollary 3.4. If D is a finite-dimensional central division algebra over the field F, then any maximal subfield K of D splits D.

PROOF. This is the special case of Theorem 3.3 in which $A = D$. The formula for the dimensions holds by Corollary 2.47. □

Corollary 3.5. If F is a field, then the Brauer group $\mathcal{B}(F)$ is the union of all relative Brauer groups $\mathcal{B}(K/F)$ as K ranges over all finite extensions of F.

REMARKS. This result is all very tidy but is not very useful, since we have no indication how to identify $\mathcal{B}(K/F)$ for a general finite extension F. In Corollary 3.9 below, we sharpen this result to make K range only over the finite *Galois* extensions of F, and we shall see in Section 3 that $\mathcal{B}(K/F)$ can be realized for such fields K in terms of the cohomology of groups.

PROOF. Any member of $\mathcal{B}(F)$ has some central division algebra D as a representative, and Corollary 3.4 identifies an extension field K of F that splits D, namely any maximal subfield of D. □

Corollary 3.6. Let D be a finite-dimensional central division algebra over a field F, and let $\dim_F D = n^2$. If K is a splitting field for D, then $\dim_F K$ is a multiple of n.

PROOF. If K is a splitting field for D, then Theorem 3.3 says that there exists an integer r such that $M_r(D)$ contains a subfield K' isomorphic to K with $\dim_F M_r(D) = (\dim_F K')^2$. Thus $r^2n^2 = (\dim_F K)^2$, and $rn = \dim_F K$. □

Theorem 3.7 (Noether–Jacobson Theorem). If D is a noncommutative finite-dimensional central division algebra over the field F, then there exists a member of D that is not in F and is separable over F.

REMARKS. Within a field extension K/F, we know from Corollary 9.31 of *Basic Algebra* that the subset of all elements of K that are separable over F is a subfield of K containing F. Consequently an equivalent formulation of the theorem is that D contains a nontrivial separable extension field of F.

PROOF (Herstein). Arguing by contradiction, suppose that no element of D outside F is separable over F. Let the characteristic of F be p, necessarily nonzero. If a is any element of D not in F, then the assumed nonseparability implies that the minimal polynomial $f(X)$ of a over F has $f'(X) = 0$, according to Proposition 9.27 of *Basic Algebra*. Hence $f(X) = f_1(X^p)$ for some polynomial $f_1(X)$ in $F[X]$. In turn, the minimal polynomial of a^p is $f_1(X)$, and if a^p is not in F, then $f_1(X) = f_2(X^p)$ for some polynomial $f_2(X)$ in $F[X]$. Since the degree decreases at each step as we pass from f to f_1, from f_1 to f_2, and so on, we conclude that a^{p^e} is in F for some e. In short, each a in D has the property that there is some integer $e \geq 0$ depending on a such that a^{p^e} is in F.

In view of the assumption that $D \neq F$ and the argument that we have just seen, there exists an element a in D outside F such that a^p is in F. Define a function $d : D \to D$ by $d(x) = xa - ax$. The function d is F linear, and it is not identically 0 because a is not in the center F of D. If r and l denote right and left multiplication, we can rewrite d as $d(x) = (r(a) - l(a))(x)$. The linear maps $r(a)$ and $l(a)$ commute with each other, and thus the Binomial Theorem is applicable in computing $d^p(x)$ as

$$d^p(x) = (r(a) - l(a))^p(x) = (r(a)^p - l(a)^p)(x) = xa^p - p^a x = 0,$$

the last equality holding because a^p is in F and is therefore central. Since d^p is the zero function and d is not, there exist an integer s with $2 \leq s \leq p$ and an element y in D with $d^{s-1}y \neq 0$ and $d^s y = 0$. Put $x = d^{s-1}y$. Since $x = d(d^{s-2}y)$, the element $w = d^{s-2}y$ has the property that $x = wa - aw$. The condition $dx = 0$ says that $xa = ax$. Put $x = au$. The elements a and u commute because a and x commute. If we set $c = wu^{-1}$, then $x = wa - aw = cua - acu$, and hence $a = xu^{-1} = cuau^{-1} - ac$. Since a and u commute, we obtain $a = ca - ac$. Right multiplying by a^{-1} gives $1 = c - aca^{-1}$ and therefore $c = 1 + aca^{-1}$. Raising both sides to the $p^{e'}$ power gives $c^{p^{e'}} = 1 + ac^{p^{e'}}a^{-1}$. The first paragraph of the proof shows that there is some $e' \geq 0$ for which $c^{p^{e'}}$ is in F, and for this integer e', we obtain the contradictory equation $c^{p^{e'}} = 1 + c^{p^{e'}}$ from the commutativity of a with F. This completes the proof. □

Corollary 3.8. If D is a noncommutative finite-dimensional central division algebra over the field F and if K is a subfield of D that is separable over F, then there exists a maximal subfield L of D containing K such that L is separable over F.

PROOF. Because of the finite dimensionality, we may assume without loss of generality that K is not properly contained in any larger subfield of D that is separable over F. Arguing by contradiction, we may assume that K is not a maximal subfield of D. Let E be the centralizer of K in D. This is a division algebra over F. It is simple by the Double Centralizer Theorem (Theorem 2.43), and it contains K because K is commutative. Moreover, we know from Theorem 2.43 that

$$\dim_F D = (\dim_F K)(\dim_F E)$$

and that K is the centralizer of E. The latter condition shows that the division algebra E is central simple over K. Since K is not a maximal subfield of D, Corollary 2.46 gives $\dim_F D > (\dim_F K)^2$. Thus $\dim_F K < \dim_F E$. Since E is central over K, E is noncommutative.

Application of Theorem 3.7 produces an element x in E outside K that is separable over K. Let L be the subfield $K(x)$ of E. Since K is a separable extension of F, the Theorem of the Primitive Element gives an element α of K such that $K = F(\alpha)$. Then $L = F(\alpha, x)$. The implication (b) implies (c) in Corollary 9.29 of *Basic Algebra* shows that if α is separable over F and x is separable over $F(\alpha)$, then α and x are both separable over F. The elements of L that are separable over F form a subfield of L, and we have just proved that this subfield properly contains K. This conclusion contradicts the assumption that K is a maximal separable extension of F within D, and the proof is complete. □

Corollary 3.9. If F is a field, then the Brauer group $\mathcal{B}(F)$ is the union of all relative Brauer groups $\mathcal{B}(K/F)$ as K ranges over all finite *Galois* extensions of F.

REMARKS. This is the result of interest. Each $\mathcal{B}(K/F)$ with K as in the corollary will be seen to be given as an H^2 in the cohomology of groups, and this group is in principle manageable. Thus we obtain a handle on $\mathcal{B}(F)$.

PROOF. If D is a central division algebra over F, then Corollaries 3.4 and 3.8 together show that some finite separable extension K' of F splits D. That is, the Brauer equivalence class of D lies in $\mathcal{B}(K'/F)$. Let us write $K' = F(\alpha)$ by the Theorem of the Primitive Element. If $f(X)$ is the minimal polynomial of α over F, then every root of $f(X)$ in an algebraic closure $\overline{F}$ of F containing K' is separable over F. Let K be the subfield of $\overline{F}$ generated by all the roots. This is a finite normal extension, and Corollary 9.30 of *Basic Algebra* shows that it is a separable extension. We have seen that the composition of the homomorphisms $\mathcal{B}(F) \to \mathcal{B}(K')$ and $\mathcal{B}(K') \to \mathcal{B}(K)$ is $\mathcal{B}(F) \to \mathcal{B}(K)$, and consequently $\mathcal{B}(K'/F) \subseteq \mathcal{B}(K/F)$. Therefore the Brauer equivalence class of D lies in $\mathcal{B}(K/F)$. □

2. Factor Sets

Throughout this section let K/F be a finite Galois extension of fields. Our objective is to construct a function from the relative Brauer group $\mathcal{B}(K/F)$ into the cohomology group $H^2(\mathrm{Gal}(K/F), K^\times)$. In Section 3 we shall prove that this function is a group isomorphism.

We take as known the material in Chapter VII of *Basic Algebra* on cohomology of groups. For convenient reference we list the relevant formulas for cohomology in degree 2. If G is a group and N is an abelian group on which G acts by automorphisms, the group $C^2(G, N)$ of 2-cochains is the group of all functions $a : G \times G \to N$, the group $Z^2(G, N)$ of 2-cocycles is the set of members f of $C^2(G, N)$ such that

$$u(f(v, w)) + f(u, vw) = f(uv, w) + f(u, v) \qquad \text{for all } u, v, w \in G,$$

the group $B^2(G, N)$ of 2-coboundaries is the set of members f of $C^2(G, N)$ of the form

$$f(u, v) = u(\alpha(v)) - \alpha(uv) + \alpha(u) \qquad \text{for some } \alpha : G \to N,$$

and the cohomology group $H^2(G, N)$ is the quotient

$$H^2(G, N) = Z^2(G, N)/B^2(G, N).$$

Here it is understood that we are using additive notation for the group operation in N and that the action of $u \in G$ on a member n of N is denoted by $u(n)$.

In constructing the function from $\mathcal{B}(K/F)$ into $H^2(\mathrm{Gal}(K/F), K^\times)$, we shall proceed in somewhat the same fashion as for the identification of group extensions with an H^2 that was carried out in Chapter VII of *Basic Algebra*. Namely we shall associate a "factor set" to some choices concerning a given finite-dimensional central simple algebra and see that this factor set is a cocyle. Then we shall show that the factor set for any set of choices for any Brauer-equivalent central simple algebra differs from this cocyle by a coboundary. The result will be the desired function from $\mathcal{B}(K/F)$ into $H^2(\mathrm{Gal}(K/F), K^\times)$.

Thus write G for $\mathrm{Gal}(K/F)$, fix a Brauer equivalence class X in $\mathcal{B}(K/F)$, and let A be a central simple algebra in the class X meeting the conditions of Theorem 3.3: A contains a subfield K' isomorphic to K, and $\dim_F A = (\dim_F K')^2$. Write $c \mapsto c'$ for the isomorphism $K \to K'$.

Let σ be an element of the Galois group G. Then $c \mapsto c'$ and $c \mapsto \sigma(c)'$ are two algebra homomorphisms of the simple algebra K into the central simple algebra A, and the Skolem–Noether Theorem (Theorem 2.41) says that they are related by an inner automorphism:

$$\boxed{\sigma(c)' = x_\sigma c' x_\sigma^{-1}} \qquad \text{for some } x_\sigma \in A.$$

Some choice is involved in selecting x_σ, but the element x_σ is unique up to a factor from K' on the right. In fact, if x_σ and y_σ both behave as in the boxed formula, then $y_\sigma^{-1} x_\sigma$ commutes with K' and hence is in K'. Thus $x_\sigma = y_\sigma c_0'$ with c_0' in K'.

The nonuniqueness can be expressed also in terms of a factor from K' on the left. In fact, the boxed formula for $c = c_0$ implies that $x_\sigma = (x_\sigma c_0' x_\sigma^{-1})(x_\sigma c_0^{-1}) = \sigma(c_0)' y_\sigma$.

At any rate, fix a choice of x_σ for all $\sigma \in G$, and let us examine the effect of composition. If σ and τ are in G, then

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

Using the result of the previous paragraph, we see that $x_{\sigma\tau}$ and $x_\sigma x_\tau$ are related by a factor from K' on the *left*. Hence we can write

$$\boxed{x_\sigma x_\tau = a(\sigma,\tau)' x_{\sigma\tau}} \qquad \text{with } a(\sigma,\tau) \in K^\times.$$

If we examine the effect of composing three elements of G, we obtain a consistency condition that the function $a : G \times G \to K^\times$ must satisfy. Namely, let ρ, σ, and τ be in G, and let us compute $x_\rho x_\sigma x_\tau$ in two ways, taking advantage of the associativity in A. With one grouping, we obtain

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

and with the other grouping, we have

$$\begin{aligned} x_\rho x_\sigma x_\tau &= x_\rho (x_\sigma x_\tau) = x_\rho a(\sigma,\tau)' x_{\sigma\tau} \\ &= \rho(a(\sigma,\tau))' x_\rho x_{\sigma\tau} = \rho(a(\sigma,\tau))' a(\rho,\sigma\tau)' x_{\rho\sigma\tau}. \end{aligned}$$

Therefore the function $a : G \times G \to K^\times$ satisfies

$$\boxed{\rho(a(\sigma,\tau)) a(\rho,\sigma\tau) = a(\rho,\sigma) a(\rho\sigma,\tau).}$$

A function $a : G \times G \to K^\times$ satisfying the above boxed formula is called a **factor set**. From A, an isomorphism $K \to K'$, and a choice of the elements x_σ for $\sigma \in G$, we have obtained a factor set.

Comparing this boxed formula with the formulas in the second paragraph of this section, we see that a factor set is exactly a member of $Z^2(\mathrm{Gal}(K/F), K^\times)$ except that the boxed formula uses multiplicative notation for $K^\times$ and the definition of 2-cocyle uses additive notation. Thus we have associated a member of $Z^2(\mathrm{Gal}(K/F), K^\times)$ to the triple consisting of A, an isomorphism $K \to K'$, and a choice of the elements x_σ for $\sigma \in G$.

With the extension K/F and the class $X \in \mathcal{B}(K/F)$ fixed, let us see the effect on the factor set of making different choices. The algebra A lies in the Brauer equivalence class X and has $\dim_F A = (\dim_F K)^2$. As we saw in the remarks with Theorem 3.3, A is determined up to isomorphism by these properties.

Thus let us start from a different system of choices: an algebra B in the class X, an isomorphism $K \to K''$, and elements y_σ for $\sigma \in G$ such that $\sigma(c)'' = y_\sigma c'' y_\sigma^{-1}$. Define the corresponding factor set $b : G \times G \to K^\times$ by

$$y_\sigma y_\tau = b(\sigma, \tau)'' y_{\sigma\tau}.$$

We wish to relate $a(\sigma, \tau)$ and $b(\sigma, \tau)$. We have just seen that A and B are isomorphic as algebras. Let $\varphi : A \to B$ be an isomorphism. Then $c \mapsto c' \mapsto \varphi(c')$ and $c \mapsto c''$ are two algebra homomorphisms of K into B, and the Skolem–Noether Theorem (Theorem 2.41) produces an element $t \in B$ with

$$c'' = t\varphi(c')t^{-1} \qquad \text{for all } c \in K.$$

Starting from the formula $\sigma(c)' = x_\sigma c' x_\sigma^{-1}$, apply φ and conjugate by t to obtain

$$\sigma(c)'' = t\varphi(\sigma(c)')t^{-1} = \big(t\varphi(x_\sigma)t^{-1}\big)c''\big(t\varphi(x_\sigma)t^{-1}\big)^{-1}.$$

This equation says that $t\varphi(x_\sigma)t^{-1}$ serves the same purpose as y_σ, and therefore

$$y_\sigma = c''_\sigma t\varphi(x_\sigma)t^{-1}$$

for some member c''_σ of K'' placed on the left. Substitution into the formula $y_\sigma y_\tau = b(\sigma, \tau)'' y_{\sigma\tau}$ gives

$$c''_\sigma t\varphi(x_\sigma)t^{-1} c''_\tau t\varphi(x_\tau)t^{-1} = b(\sigma, \tau)'' c''_{\sigma\tau} t\varphi(x_{\sigma\tau})t^{-1}.$$

If we substitute from the formula $c'' = t\varphi(c')t^{-1}$ for all members of K'' and then conjugate by t^{-1} and apply φ^{-1}, we obtain

$$c'_\sigma x_\sigma c'_\tau x_\tau = b(\sigma, \tau)' c'_{\sigma\tau} x_{\sigma\tau}.$$

The left side equals

$$c'_\sigma \sigma(c_\tau)' x_\sigma x_\tau = c'_\sigma \sigma(c_\tau)' a(\sigma, \tau)' x_{\sigma\tau},$$

and comparison of this expression with the right side gives

$$b(\sigma,\tau)'c'_{\sigma\tau} = c'_\sigma\sigma(c_\tau)'a(\sigma,\tau)'.$$

Passing from K' back to K, we conclude that

$$\boxed{b(\sigma,\tau)c_{\sigma\tau} = c_\sigma\sigma(c_\tau)a(\sigma,\tau).}$$

This formula says that b is the product of a and the **trivial factor set** $c : G \times G \to K^\times$ given by

$$c(\sigma,\tau) = c_\sigma\sigma(c_\tau)c_{\sigma\tau}^{-1},$$

where $\sigma \mapsto c_\sigma$ is some function from G to $K^\times$. Again referring to the second paragraph of this section and remembering that we are using multiplicative notation for $K^\times$, we see that the trivial factor sets are the 2-coboundaries, lying in $B^2(\mathrm{Gal}(K/F), K^\times)$, in the same way that the general factor sets are the 2-cocycles, lying in $Z^2(\mathrm{Gal}(K/F), K^\times)$. We have thus proved the following proposition.

Proposition 3.10. Let K be a finite Galois extension of the field F. For X in $\mathcal{B}(K/F)$, let A be an algebra in the Brauer equivalence class X with $\dim_F A = (\dim_F K)^2$, let $K \to K'$ be an isomorphism of K into A, and let $\{x_\sigma \mid \sigma \in \mathrm{Gal}(K/F)\} \subseteq A^\times$ be a set of elements such that $\sigma(c)' = x_\sigma c' x_\sigma^{-1}$. Then the passage from X to the factor set determined by the triple of data $(A,\ K \to K',\ \{x_\sigma\})$ descends to a well-defined function from the abelian group $\mathcal{B}(K/F)$ to the abelian group $H^2(\mathrm{Gal}(K/F), K^\times)$.

3. Crossed Products

In this section we continue to assume that K/F is a finite Galois extension of fields. We are going to show that the function $\mathcal{B}(K/F) \to H^2(\mathrm{Gal}(K/F), K^\times)$ given in Proposition 3.10 is an isomorphism of groups. The homomorphism property comes last and is the hard part of the argument. In the meantime, we construct the inverse function by associating an algebra to each member of $Z^2(\mathrm{Gal}(K/F), K^\times)$ and showing in Corollary 3.13 that the resulting function on $Z^2(\mathrm{Gal}(K/F), K^\times)$ descends to an inverse function from $H^2(\mathrm{Gal}(K/F), K^\times)$ into $\mathcal{B}(K/F)$. The algebra is called a “crossed product” and is produced in Proposition 3.12 below. Before either of these steps, we establish one more property of the system $\{x_\sigma \mid \sigma \in \mathrm{Gal}(K/F)\}$ of the previous section that has not needed mentioning until now.

Thus let a central simple algebra A be given with $\dim_F A = (\dim_F K)^2$, along with an isomorphism $K \to K'$ denoted by $c \mapsto c'$. As in the previous section we choose $x_\sigma \in A^\times$ with

$$\sigma(c)' = x_\sigma c' x_\sigma^{-1} \qquad \text{for all } c \in K.$$

The corresponding factor set $a(\sigma, \tau)$ has

$$x_\sigma x_\tau = a(\sigma, \tau)' x_{\sigma\tau}.$$

We regard A as a vector space over K' with K' acting by multiplication on the left.

Lemma 3.11. With hypotheses as above, the set $\{x_\sigma \mid \sigma \in \mathrm{Gal}(K/F)\}$ is a vector-space basis of A over K'.

PROOF. Let $G = \mathrm{Gal}(K/F)$. Since $|G| = \dim_F K = \dim_F K' = \dim_{K'} A$, it is enough to prove linear independence. Arguing by contradiction, assume that the set $\{x_\sigma \mid \sigma \in G\}$ is linearly dependent. Choose a maximal subset J of G such that $\{x_\tau \mid \tau \in J\}$ is linearly independent. For σ not in J, we then have

$$x_\sigma = \sum_{\tau \in J} a'_\tau x_\tau \qquad \text{with } a_\tau \in K. \tag{$*$}$$

Every c in K satisfies

$$\sigma(c)' x_\sigma = x_\sigma c' = \sum_{\tau \in J} a'_\tau x_\tau c' = \sum_{\tau \in J} a'_\tau \tau(c)' x_\tau,$$

and thus $x_\sigma = \sum_{\tau \in J} \sigma(c)'^{-1} a'_\tau \tau(c)' x_\tau$. Comparing this expansion with $(*)$ shows that

$$\sigma(c)'^{-1} a'_\tau \tau(c)' = a'_\tau \qquad \text{for } \tau \in J. \tag{$**$}$$

Since $x_\sigma \neq 0$, some a'_τ in the expansion $(*)$ is nonzero. For this τ, we can cancel a'_τ in $(**)$ and obtain $\sigma(c)' = \tau(c)'$ for all $c \in K$. Then $\sigma = \tau$, in contradiction to the fact that σ is not in J. □

The linear independence in Lemma 3.11 allows us to read off the structure of A: as a K' vector space, the algebra A is given by $A = \bigoplus_{\sigma \in \mathrm{Gal}(K/F)} K' x_\sigma$, and the elements x_σ have the properties that

$$x_\sigma c' = \sigma(c)' x_\sigma \ \text{ for } c \in K \qquad \text{and} \qquad x_\sigma x_\tau = a(\sigma, \tau)' x_{\sigma\tau}.$$

Proposition 3.12 is motivated by these formulas, saying that we can reconstruct A from a given 2-cocycle $a(\sigma, \tau)$ in such a way that these formulas hold.

Proposition 3.12. Let K/F be a finite Galois extension, and let $a = a(\sigma, \tau)$ be in $Z^2(\mathrm{Gal}(K/F), K^\times)$. Then there exist a central simple algebra A over F with $\dim_F A = (\dim_F K)^2$, an isomorphism $K \to K'$ of K onto a subfield K' of A, and a subset $\{x_\sigma \in A \mid \sigma \in \mathrm{Gal}(K/F)\}$ such that

(a) $A = \bigoplus_{\sigma \in \mathrm{Gal}(K/F)} K' x_\sigma$,

(b) $x_\sigma c' x_\sigma^{-1} = \sigma(c)'$ for all c in K, with $c \mapsto c'$ denoting the isomorphism of K onto K',

(c) $x_\sigma x_\tau = a(\sigma, \tau)' x_{\sigma\tau}$.

REMARKS. We write $A = \mathcal{A}(K, \mathrm{Gal}(K/F), a)$ and call A the **crossed-product algebra** corresponding to the factor set a. The algebra A is completely determined by the given conditions, up to canonical isomorphism, since (a), (b), and (c) determine the entire multiplication table of A.

PROOF. Let $G = \mathrm{Gal}(K/F)$, form a set $\{x_\sigma \mid \sigma \in G\}$, and let A be the K vector space (free K module) with basis $\{x_\sigma\}$. Then $A = \bigoplus_{\sigma \in G} K x_\sigma$. Define a multiplication on K basis vectors in A by

$$(c x_\sigma)(d x_\tau) = c\sigma(d) a(\sigma, \tau) x_{\sigma\tau}, \tag{$*$}$$

and extend it to a multiplication on A by additivity.

First we shall check that A is an associative F algebra with $a(1,1)^{-1}x_1$ as identity by making use of the cocycle property

$$\rho(a(\sigma, \tau)) a(\rho, \sigma\tau) = a(\rho, \sigma) a(\rho\sigma, \tau). \tag{$**$}$$

For associativity, $(*)$ gives

$$\begin{aligned}(b x_\rho)\big((c x_\sigma (d x_\tau)\big) &= (b x_\rho)(c\sigma(d) a(\sigma, \tau) x_{\sigma\tau}) \\ &= b\rho(c)(\rho\sigma(d))\rho(a(\sigma, \tau)) a(\rho, \sigma\tau) x_{\rho\sigma\tau}\end{aligned}$$

and

$$\begin{aligned}\big((b x_\rho)(c x_\sigma\big)(d x_\tau) &= (b\rho(c) a(\rho, \sigma) x_{\rho\sigma})(d x_\tau) \\ &= b\rho(c) a(\rho, \sigma)\rho\sigma(d)) a(\rho\sigma, \tau) x_{\rho\sigma\tau},\end{aligned}$$

and the right sides are equal by $(**)$. To see that $a(1,1)^{-1}x_1$ is a two-sided identity, take $\rho = \sigma = 1$ in $(**)$ to get $1(a(1, \tau)) a(1, \tau) = a(1,1) a(1, \tau)$. Since a takes values in $K^\times$, we can cancel and obtain

$$a(1, \tau) = a(1, 1). \tag{$\dagger$}$$

Thus $(*)$ gives

$$\big(a(1,1)^{-1} x_1\big)(d x_\tau) = a(1,1)^{-1} 1(d) a(1, \tau) x_\tau = d x_\tau.$$

Similarly another specialization of $(**)$ is $\sigma(a(1,1))a(\sigma,1) = a(\sigma,1)a(\sigma,1)$, from which we obtain

$$\sigma(a(1,1)) = a(\sigma,1). \tag{$\dagger\dagger$}$$

Thus $(*)$ gives

$$(cx_\sigma)\big(a(1,1)^{-1}x_1\big) = c\sigma(a(1,1))^{-1}a(\sigma,1)x_\sigma = cx_\sigma,$$

and $a(1,1)^{-1}x_1$ is indeed a two-sided identity. We denote it by 1. Scalar multiplication by $r \in F$ is understood to be the additive extension of $r(cx_\sigma) = (rc)x_\sigma$ for $c \in K$, and the identities

$$\begin{aligned}\big(r(cx_\sigma)\big)(dx_\tau) &= rc\sigma(d)a(\sigma,\tau)x_{\sigma\tau},\\ (cx_\sigma)\big(r(dx_\tau)\big) &= c\sigma(rd)a(\sigma,\tau)x_{\sigma\tau} = rc\sigma(d)a(\sigma,\tau)x_{\sigma\tau},\\ r\big((cx_\sigma)(dx_\tau)\big) &= rc\sigma(d)a(\sigma,\tau)x_{\sigma\tau}\end{aligned}$$

show that multiplication in A is F linear with respect to scalars, hence show that A is an algebra over F.

Second we define $K' \subseteq A$ and an isomorphism $K \to K'$. For $b \in K$, we let b' be the member of A given by $b' = b1 = b(a(1,1)^{-1}x_1)$, and we let K' be the image of K under $b \mapsto b'$. The map $b \mapsto b'$ certainly respects addition, and it respects multiplication because the identity

$$(b_1a(1,1)^{-1}x_1)(b_2a(1,1)^{-1}x_1) = b_1b_2a(1,1)^{-1}x_1$$

is immediate from $(*)$. Hence K' is a subfield of A.

Third we prove properties (a), (b), and (c). For (a), we use $(*)$ and $(\dagger)$ to obtain the identity

$$b'x_\sigma = (ba(1,1)^{-1}x_1)x_\sigma = ba(1,1)^{-1}a(1,\sigma)x_\sigma = bx_\sigma. \tag{$\ddagger$}$$

This identity shows that $K'x_\sigma = Kx_\sigma$, and (a) follows. From $(\ddagger)$, we see also that $x_\sigma(bx_{\sigma^{-1}}) = (1x_\sigma)(bx_{\sigma^{-1}}) = 1\sigma(b)a(\sigma,\sigma^{-1})x_1$ and that $(bx_{\sigma^{-1}})x_\sigma = b\sigma(1)a(\sigma^{-1},\sigma)x_1$; thus x_σ has a right inverse in A and also a left inverse, hence a two-sided inverse. Consequently the statement of (b) is meaningful; for its proof we have only to observe that

$$\begin{aligned}x_\sigma c'x_\sigma^{-1} &= \big(x_\sigma(ca(1,1)^{-1}x_1)\big)x_\sigma^{-1} = \big(\sigma(c)\sigma(a(1,1))^{-1}a(\sigma,1)x_\sigma\big)\cdot x_\sigma^{-1}\\ &= \sigma(c)x_\sigma \cdot x_\sigma^{-1} = \sigma(c)'x_\sigma x_\sigma^{-1} = \sigma(c)',\end{aligned}$$

the last three equalities following from $(\dagger\dagger)$, $(\ddagger)$, and the identity $x_\sigma x_\sigma^{-1} = 1$. For (c), we have

$$x_\sigma x_\tau = a(\sigma,\tau)x_{\sigma\tau} = a(\sigma,\tau)'x_{\sigma\tau},$$

the second equality following from (‡).

Fourth we show that A is simple. Let I be a proper two-sided ideal in A, and let $\varphi : A \to A/I$ be the quotient homomorphism. Since 1 is not in I and since K' is a subfield of A, we know that $\ker(\varphi\big|_{K'}) = 0$ and that $\varphi(K')$ is a subfield of A/I. The field $\varphi(K')$ acts on A/I by left multiplication and makes A/I into a $\varphi(K')$ vector space. The members $\varphi(x_\sigma)$ of A/I certainly span A/I over $\varphi(K')$ because of (a), and the claim is that they are linearly independent. If so, then φ is one-one, I equals 0, and A is simple. For the linear independence, we argue by contradiction in the same way as for Lemma 3.11. Suppose that $J \subseteq G$ is a maximal subset such that $\{\varphi(x_\tau) \mid \tau \in J\}$ is linearly independent over $\varphi(K')$. For σ not in J, we then have

$$\varphi(x_\sigma) = \sum_{\tau \in J} \varphi(a'_\tau)\varphi(x_\tau) \qquad \text{with } a_\tau \in K. \tag{‡‡}$$

Every c in K satisfies

$$\varphi(\sigma(c)')\varphi(x_\sigma) = \varphi(x_\sigma)\varphi(c') = \sum_{\tau \in J} \varphi(a'_\tau)\varphi(x_\tau)\varphi(c') = \sum_{\tau \in J} \varphi(a'_\tau)\varphi(\tau(c)')\varphi(x_\tau),$$

and thus

$$\varphi(x_\sigma) = \textstyle\sum_{\tau \in J} \varphi(\sigma(c)')^{-1}\varphi(a'_\tau)\varphi(\tau(c)')\varphi(x_\tau).$$

Comparing this expansion with (‡‡) shows that

$$\varphi(\sigma(c)')^{-1}\varphi(a'_\tau)\varphi(\tau(c)') = \varphi(a'_\tau) \qquad \text{for } \tau \in J. \tag{§}$$

Since x_σ is invertible in A, $\varphi(x_\sigma)$ is invertible in A/I and cannot be 0. Therefore some $\varphi(a'_\tau)$ in the expansion (‡‡) is nonzero. For this τ, we can cancel $\varphi(a'_\tau)$ in (§) and obtain $\varphi(\sigma(c)') = \varphi(\tau(c)')$ for all $c \in K$. Since φ is one-one on K', we conclude that $\sigma = \tau$, in contradiction to the fact that σ is not in J. Therefore A is simple.

Fifth we show that A has center F. Thus suppose that $\sum_\sigma c'_\sigma x_\sigma$ is central. Commutativity with $d'x_\tau$ forces the two expressions

$$\big(\sum_\sigma c'_\sigma x_\sigma\big)d'x_\tau = \sum_\sigma c'_\sigma \sigma(d)' x_\sigma x_\tau = \sum_\sigma c'_\sigma \sigma(d)' a(\sigma,\tau)' x_{\sigma\tau}$$

and

$$\begin{aligned} d'x_\tau\big(\sum_\sigma c'_\sigma x_\sigma\big) &= \sum_\sigma (d'x_\tau)(c'_\sigma x_\sigma) = \sum_\sigma d'\tau(c_\sigma)' a(\tau,\sigma)' x_{\tau\sigma} \\ &= \sum_\sigma d'\tau(c_{\tau^{-1}\sigma\tau})' a(\tau, \tau^{-1}\sigma\tau)' x_{\sigma\tau} \end{aligned}$$

to be equal. Hence

$$d\tau(c_{\tau^{-1}\sigma\tau})a(\tau,\tau^{-1}\sigma\tau) = c_\sigma \sigma(d) a(\sigma,\tau) \qquad \text{for all } d, \sigma, \tau. \tag{§§}$$

Putting $d = 1$ in (§§) shows that $\tau(c_{\tau^{-1}\sigma\tau})a(\tau, \tau^{-1}\sigma\tau) = c_\sigma a(\sigma, \tau)$. Substituting from this equation into the left side of (§§) gives

$$dc_\sigma a(\sigma, \tau) = c_\sigma \sigma(d)a(\sigma, \tau) \qquad \text{for all } d, \sigma, \tau.$$

If $c_\sigma \neq 0$, we see that $\sigma(d) = d$ for all $d \in K$; thus $c_\sigma \neq 0$ only for $\sigma = 1$. For $\sigma = 1$ and $d = 1$, (§§) reduces to

$$\tau(c_1)a(\tau, 1) = c_1 a(1, \tau).$$

Taking into account (†) and (††), we obtain

$$\tau(c_1 a(1, 1)) = c_1 a(1, 1).$$

Since τ is arbitrary, this says that $c_1 a(1, 1)$ is in F. Thus the central element is $c_1' x_1 = c_1 x_1 = c_1 a(1, 1)a(1, 1)^{-1} x_1 = (c_1 a(1, 1))1$ and is an F multiple of the identity.

Since $\{x_\sigma\}$ by definition is a basis of A over K, we have $\dim_K A = |G| = \dim_F K$. Multiplying this equation by $\dim_F K$ yields $\dim_F A = (\dim_F K)^2$. This completes the proof. □

Corollary 3.13. If K is a finite Galois extension of the field F, then the map $\mathcal{B}(K/F) \to H^2(\mathrm{Gal}(K/F), K^\times)$ defined via factor sets is one-one onto.

PROOF. Put $G = \mathrm{Gal}(K/F)$. If $a : G \times G \to K^\times$ is in $Z^2(G, K^\times)$, then we can construct an algebra A via Proposition 3.12, and the claim is that the map $a \mapsto A$ descends to $H^2(G, K^\times)$ and is a two-sided inverse to the map from $\mathcal{B}(K/F)$ into $H^2(G, K^\times)$ given in Proposition 3.10.

First we show that $a \mapsto A$ descends to $H^2(G, K^\times)$. Thus suppose that b is a second cocycle and is of the form $b(\sigma, \tau) = a(\sigma, \tau)c_\sigma \sigma(c_\tau)c_{\sigma\tau}^{-1}$, i.e., represents the same member of $H^2(G, K^\times)$. Let B be the algebra constructed from b by Proposition 3.12, say with K mapping to $K'' \subseteq B$ via $c \mapsto c''$ and with

(a′) $B = \bigoplus_{\sigma \in G} K'' y_\sigma$ for a subset $\{y_\sigma\}$ of B,
(b′) $y_\sigma c'' y_\sigma^{-1} = \sigma(c)''$,
(c′) $y_\sigma y_\tau = b(\sigma, \tau)'' y_{\sigma\tau}$.

Define $\varphi : A \to B$ to be the additive extension of the function with $\varphi(c' x_\sigma) = c'' c_\sigma''^{-1} y_\sigma$. To check that φ is an algebra homomorphism, we start from the formula $(c' x_\sigma)(d' x_\tau) = c' \sigma(d)' a(\sigma, \tau)' x_{\sigma\tau}$ and apply φ to obtain

$$\varphi\big((c' x_\sigma)(d' x_\tau)\big) = c'' \sigma(d)'' a(\sigma, \tau)'' c_{\sigma\tau}''^{-1} y_{\sigma\tau}.$$

Meanwhile,

$$\begin{aligned}\varphi(c'x_\sigma)\varphi(d'x_\tau) &= (c''c''^{-1}_\sigma y_\sigma)(d''c''^{-1}_\tau y_\tau)\\ &= c''c''^{-1}_\sigma\sigma(d)''\sigma(c_\tau)''^{-1}b(\sigma,\tau)''y_{\sigma\tau}\\ &= c''c''^{-1}_\sigma\sigma(d)''\sigma(c_\tau)''^{-1}a(\sigma,\tau)''c''_\sigma\sigma(c_\tau)''c''_{\sigma\tau}{}^{-1}y_{\sigma\tau}.\end{aligned}$$

Hence $\varphi\big((c'x_\sigma)(d'x_\tau)\big) = \varphi(c'x_\sigma)\varphi(d'x_\tau)$, and φ is an algebra homomorphism. Since φ carries K basis to K basis, φ is an algebra isomorphism.

Thus the map $a \mapsto A$ descends to a map from $H^2(G, K^\times)$ into $\mathcal{B}(K/F)$. Starting from a cocycle a in $Z^2(G, K^\times)$, we can construct A and elements x_σ by Proposition 3.12, we can apply Propositions 3.12b and 3.10 to the x_σ's to obtain another cocycle $\bar{a}$ in $Z^2(G, K^\times)$, and we can use Proposition 3.12c to see that $\bar{a} = a$. In the reverse direction if we start from an algebra A, make a set of choices, and form a factor set a by means of Proposition 3.10, then Proposition 3.12 constructs an algebra $\overline{A}$ that has to be isomorphic to A because conditions (a) through (c) in Proposition 3.12 determine the same multiplication table for an algebra as was used in constructing the cocycle a. □

Theorem 3.14. If K is a finite Galois extension of the field F, then the map $\mathcal{B}(K/F) \to H^2(\mathrm{Gal}(K/F), K^\times)$ defined via factor sets is a group isomorphism.

REMARKS. Put $G = \mathrm{Gal}(K/F)$. In view of Corollary 3.13, is enough to prove that the mapping $Z^2(G, K^\times) \to \mathcal{B}(K/F)$ of Proposition 3.12 is a group homomorphism. Thus let A, B, and C be the crossed-product algebras $A = \mathcal{A}(K, G, a)$, $B = \mathcal{A}(K, G, b)$, and $C = \mathcal{A}(K, G, ab)$. We are to prove that $A \otimes_F B$ is Brauer equivalent to C. Each of A, B, and C has F dimension $(\dim_F K)^2$, and hence $A \otimes_F B$ will not be isomorphic to C. Consequently we need to prove Brauer equivalence of two specific nonisomorphic algebras. This is the circumstance that makes the proof complicated.

PROOF (Chase). Let G, a, b, A, B, and C be as in the remarks. We can regard A and B as vector spaces over K with K acting on the left in each case. We define an F vector space M to be the quotient of $A \otimes_F B$ by the F vector subspace I generated by all vectors $ca \otimes b - a \otimes cb$ with $a \in A$, $b \in B$, and $c \in K$. We write $M = A \otimes_K B$ for this quotient, even though more standard notation for it might be $A^o \otimes_K B$ with A^o as a right K module and B as a left K module.

The subspace I is carried to itself by right multiplication by any member of the algebra $A \otimes_F B$ and hence is a right ideal. The quotient M is therefore a unital right $A \otimes_F B$ module with $(a \otimes_K b)(a' \otimes_F b') = aa' \otimes_K bb'$ for $a \otimes_K b$ in M and $a' \otimes_F b'$ in $A \otimes_F B$.

We shall make the unital right $A \otimes_F B$ module M into a unital $(C, A \otimes_F B)$ bimodule by introducing an action by C on the left. For this purpose let $\{u_\sigma\}$, $\{v_\sigma\}$, and $\{w_\sigma\}$ be the distinguished K bases of the algebras A, B, and C indexed by G and used to form A, B, and C from the 2-cocycles a, b, and ab. Given an element xw_σ in C with $x \in K$, define xw_σ on $A \otimes_F B$ to be (left by xu_σ) $\otimes$ (left by v_σ). Let us see that this operation carries the generators of I into I. We have

$$\begin{aligned}(xw_\sigma)(ca \otimes_F b) - (xw_\sigma)(a \otimes_F cb) &= xu_\sigma ca \otimes_F v_\sigma b - xu_\sigma a \otimes_F v_\sigma cb \\ &= x\sigma(c)u_\sigma a \otimes_F v_\sigma b - xu_\sigma a \otimes_F \sigma(c)v_\sigma b \\ &= \sigma(c)(xu_\sigma a) \otimes_F (v_\sigma b) \\ &\quad - (xu_\sigma a) \otimes_F \sigma(c)(v_\sigma b),\end{aligned}$$

and the right side is indeed in I. Thus we obtain an operation of xw_σ on the left for $A \otimes_K B$ such that

$$(xw_\sigma)(a \otimes_K b) = xu_\sigma a \otimes_K v_\sigma b \quad \text{for } x \in K,\ \sigma \in G,\ a \in A,\ b \in B. \qquad (*)$$

We extend this definition by additivity in such a way that all of C operates on the left for $A \otimes_K B$.

The claim is that the additive extension $(*)$ to C makes $M = A \otimes_K B$ into a unital left C module. What needs proof is that 1 acts as 1 and that

$$\big((xw_\sigma)(yw_\tau)\big)(a \otimes_K b) = (xw_\sigma)\big((yw_\tau)(a \otimes_K b)\big). \qquad (**)$$

The element 1 in C is $a(1,1)^{-1}b(1,1)^{-1}w_1$, and we have

$$\begin{aligned}\big(a(1,1)^{-1}b(1,1)^{-1}w_1\big)(a \otimes_K b) &= a(1,1)^{-1}b(1,1)^{-1}u_1 a \otimes_K v_1 b \\ &= a(1,1)^{-1}u_1 a \otimes_K b(1,1)^{-1}v_1 b = a \otimes_K b.\end{aligned}$$

Thus 1 acts as 1. For $(**)$, the left side is

$$(x\sigma(y)a(\sigma,\tau)b(\sigma,\tau)w_{\sigma\tau})(a \otimes_K b) = x\sigma(y)a(\sigma,\tau)b(\sigma,\tau)u_{\sigma\tau}a \otimes_K v_{\sigma\tau}b,$$

while the right side is

$$\begin{aligned}(xw_\sigma)(yu_\tau a \otimes_K v_\tau b) &= xu_\sigma yu_\tau a \otimes_K v_\sigma v_\tau b = x\sigma(y)u_\sigma u_\tau a \otimes_K v_\sigma v_\tau b \\ &= x\sigma(y)a(\sigma,\tau)u_{\sigma\tau}a \otimes_K b(\sigma,\tau)v_{\sigma\tau}b.\end{aligned}$$

These are equal, since $b(\sigma,\tau)$ is in K and therefore moves across the tensor-product sign.

Thus M is a unital left C module. The left action by C certainly commutes with the right action by $A \otimes_F B$, and M is consequently a unital $(C, A \otimes_F B)$ bimodule. Each member of $A \otimes_F B$ therefore yields by its right action a member of the ring $\operatorname{End}_C(M)$, and we obtain a ring homomorphism of $(A \otimes_F B)^o$ into $\operatorname{End}_C(M)$. Since $A \otimes_F B$ is a simple ring, this homomorphism is one-one. If we can prove that this homomorphism is onto, then we will have a ring isomorphism $(A \otimes_F B)^o \cong \mathrm{End}_C(M)$, and the rest will be easy.

To see that the homomorphism is onto, we shall calculate dimensions. Let $n = \dim_F K$. Then each of A, B, and C has F dimension n^2, and we have

$$\dim_F M = (\dim_F A)(\dim_F B)/(\dim_F K) = n^2n^2/n = n^3 = (\dim_F C)n.$$

Since the algebra C is simple, every unital left C module is semisimple and is in fact isomorphic to a multiple of a simple left C module V. The above dimensional equality says that if r is the integer such that C is isomorphic to rV as a left C module, then M is isomorphic to nrV.

Let D^o be the division algebra $\mathrm{End}_C(V)$. As in the proof of Wedderburn's Theorem (Theorem 2.2), we know for each integer m that

$$\mathrm{End}_C(mV) \cong M_m(\mathrm{End}_C(V)) \cong M_m(D^o). \tag{†}$$

Taking $m = r$ in (†) gives $C^o \cong \mathrm{End}_C(rV) \cong M_r(D^o)$. Hence

$$C \cong M_r(D), \tag{††}$$

and $\dim_F C = r^2 \dim_F D$. Since $\dim_F C = (\dim_F K)^2 = n^2$, we obtain $\dim_F D = n^2/r^2$. Taking $m = nr$ in (†) gives

$$\mathrm{End}_C(M) \cong \mathrm{End}_C(nrV) \cong M_{nr}(D^o), \tag{‡}$$

and we therefore obtain

$$\dim_F \mathrm{End}_C(M) = n^2r^2 \dim_F D = (n^2r^2)(n^2/r^2) = n^4.$$

Since $\dim_F(A \otimes_F B) = n^4$, we obtain $\dim_F(A \otimes_F B)^o = \dim_F \mathrm{End}_C(M)$, and we conclude that the algebra homomorphism $(A \otimes_F B)^o \to \mathrm{End}_C(M)$ is onto. Thus it is an isomorphism, and $A \otimes_F B \cong (\mathrm{End}_C(M))^o$.

Combining this isomorphism with (‡) shows that $A \otimes_F B \cong M_{nr}(D)$. In view of (††), $A \otimes_F B$ is therefore Brauer equivalent to C. □

Corollary 3.15. If D is a finite-dimensional central division algebra of dimension m^2 over a field F, then the m-fold tensor product of D with itself over F is a full matrix algebra over F.

PROOF. Corollary 3.9 produces a finite Galois extension K of F such that K splits D. Write G for $\mathrm{Gal}(K/F)$. In view of Theorems 3.3 and 2.4, there exists an integer l such that $A = M_l(D)$ contains a subfield K' isomorphic to K with $\dim_F A = (\dim_F K')^2$. Changing notation, we may redefine $K = K'$. Let

$n = \dim_F K$. Then $n^2 = \dim_F A = l^2 \dim_F D = (lm)^2$, and $n = lm$. Following the construction of factor sets in Section 2 and using Lemma 3.11, we form a vector-space basis $\{x_\sigma \mid \sigma \in G\}$ of A over K and a factor set $\{a(\sigma, \tau)\}$ such that $x_\sigma x_\tau = a(\sigma, \tau)x_{\sigma\tau}$ and $\sigma(c) = x_\sigma c x_\sigma^{-1}$ for all c in K.

Example 1 of semisimple rings in Section II.2 shows that the left A module A is the direct sum of l isomorphic simple left A modules. Let V be one of these. Restricting the module structure of V from A to K makes V into a unital left K module, hence into a vector space over K. Then we have

$$n^2 = \dim_F A = l \dim_F V = l(\dim_K V)(\dim_F K) = ln \dim_K V,$$

and $\dim_K V = m$. Let $v_1, \dots, v_m$ be a K basis of V. For each $x \in A$, define a matrix $C(x)$ in $M_m(K)$ by

$$xv_j = \sum_{i=1}^m C(x)_{ij} v_i.$$

For σ and τ in G, we compute $x_\sigma x_\tau v_i$ in two ways as

$$x_\sigma x_\tau v_j = a(\sigma, \tau)x_{\sigma\tau} v_j = a(\sigma, \tau) \sum_{i=1}^m C(x_{\sigma\tau})_{ij} v_i \tag{$*$}$$

and as

$$x_\sigma x_\tau v_j = x_\sigma \sum_{k=1}^m C(x_\tau)_{kj} v_k = \sum_{k=1}^m \sigma(C(x_\tau)_{kj}) x_\sigma v_k = \sum_{i,k=1}^m \sigma(C(x_\tau)_{kj}) C(x_\sigma)_{ik} v_i.$$

If we write $\sigma(C(x_\tau))$ for the result of applying σ to each entry of $C(x_\tau)$, then we obtain

$$x_\sigma x_\tau v_j = \sum_{i=1}^m (C(x_\sigma)\sigma(C(x_\tau))_{ij} v_i. \tag{$**$}$$

Comparing $(*)$ and $(**)$ leads to the matrix equation in $M_m(K)$ given by

$$a(\sigma, \tau)C(x_{\sigma\tau}) = C(x_\sigma)\sigma(C(x_\tau)).$$

Putting $c_\sigma = \det C(x_\sigma)$ and taking the determinant of both sides yields

$$a(\sigma, \tau)^m c_{\sigma\tau} = c_\sigma \sigma(c_\tau).$$

This equation shows that $a(\sigma, \tau)^m$ is a trivial factor set. Applying Theorem 3.14, we see that the m^{th} power of the Brauer equivalence class of A is trivial. Since A is Brauer equivalent to D, the corollary follows. □

Corollary 3.16. If F is any field, then every element of $\mathcal{B}(F)$ has finite order.

PROOF. If A is any central simple algebra over F, then Theorem 2.4 shows that $A \cong M_l(D)$ for some integer $l \geq 1$ and some central division algebra D over F. Corollary 3.15 shows that the Brauer equivalence class of D has finite order in $\mathcal{B}(F)$. Since A is Brauer equivalent to D, the same thing is true for A. □

4. Hilbert's Theorem 90

Let K/F be a finite Galois extension of fields. Our interest in this section will be in the cohomology groups $H^q(\mathrm{Gal}(K/F), K^\times)$ with q possibly different from 2. For $q = 0$, $H^0(G, N)$ is always the subgroup of elements of N fixed by every element of G. In the case of a Galois extension, the members of $K^\times$ fixed by the Galois group are the nonzero elements of the base field F. Thus we have

$$H^0(\mathrm{Gal}(K/F), K^\times) \cong F^\times.$$

In addition, Theorem 3.14 has established an isomorphism

$$H^2(\mathrm{Gal}(K/F), K^\times) \cong \mathcal{B}(K/F),$$

and thus we have already obtained some understanding of this group for $q = 2$.

We shall examine H^1 in a moment, but first we take note of another fact about H^2. Problem 16b at the end of Chapter VII of *Basic Algebra* shows that if G is a finite group and N is an abelian group on which G acts by automorphisms, then every element of $H^q(G, N)$ for $q > 0$ has order dividing $|G|$. In particular, every element of $H^2(\mathrm{Gal}(K/F), K^\times)$ has order dividing $\dim_F K$ whenever K is a finite Galois extension of F. Applying Theorem 3.14, we see that every member of $\mathcal{B}(K/F)$ has order dividing $\dim_F K$. In view of Corollary 3.9, this argument gives a new and shorter proof of the result of Corollary 3.16 that every member of $\mathcal{B}(F)$ has finite order. The estimate of the order via Corollary 3.15, however, is sharper than the estimate obtained via the shorter proof, and this distinction makes all the difference in Problem 12 at the end of the chapter.

The result concerning H^1 and its important special case given as Corollary 3.18 below are known as **Hilbert's Theorem 90**.

Theorem 3.17. If K/F is any finite Galois extension of fields, then $H^1(\mathrm{Gal}(K/F), K^\times) = 0$.

PROOF. Let $G = \mathrm{Gal}(K/F)$, put $n = \dim_F K$, and enumerate G as $\sigma_1, \dots, \sigma_n$. By the Theorem of the Primitive Element, we can write $K = F(\alpha)$ for some α in K, and then $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis of K over F. Form the n-by-n matrix M

with entries in K whose $(i,j)^{\text{th}}$ entry is $\sigma_j(\alpha^{i-1})$. This is a Vandermonde matrix, and Corollary 5.3 of *Basic Algebra* gives its determinant as $\prod_{j>i}[\sigma_j(\alpha)-\sigma_i(\alpha)]$. This determinant cannot be 0, since $\sigma_j(\alpha)=\sigma_i(\alpha)$ implies $\sigma_j(\alpha^k)=\sigma_j(\alpha)^k=\sigma_i(\alpha)^k=\sigma_i(\alpha^k)$ for all k and then $\sigma_j(x)=\sigma_i(x)$ for all x. Hence the matrix M is nonsingular.

Let f be a nonzero element in $Z^1(G,K^\times)$. Such a function $f:G\to K$ is nowhere vanishing and has $f(\sigma\tau)=f(\sigma)\sigma(f(\tau))$ for all σ and τ in G. Since the matrix M is nonsingular, the nontrivial linear combination $\sum_{\sigma\in G}f(\sigma)\sigma$ cannot be 0 on all members of the basis $\{1,\alpha,\alpha^2,\dots,\alpha^{n-1}\}$. Choose k with $\sum_{\sigma\in G}f(\sigma)\sigma(\alpha^k)=y\neq 0$. Applying $\tau\in G$ to this equation, we obtain

$$\begin{aligned}\tau(y)&=\sum_{\sigma\in G}\tau(f(\sigma))\tau\sigma(\alpha^k)=\sum_{\sigma\in G}f(\tau\sigma)f(\tau)^{-1}\tau\sigma(\alpha^k)\\&=f(\tau^{-1})\sum_{\sigma\in G}f(\sigma)\sigma(\alpha^k)=f(\tau)^{-1}y.\end{aligned}$$

The equation $f(\tau)^{-1}=\tau(y)y^{-1}$ shows that f^{-1} is a coboundary, hence that f is a coboundary. □

Corollary 3.18. If K/F is a finite Galois extension with cyclic Galois group and if σ is a generator of the Galois group, then every member x of K with $N_{K/F}(x)=1$ is of the form $x=\sigma(y)y^{-1}$ for some $y\in K^\times$.

REMARKS. The instance of this corollary in which K is a quadratic number field and F is the field $\mathbb{Q}$ appears as Problem 27 at the end of Chapter I. In subsequent problems at the end of that chapter, Problem 27 plays a crucial role in showing that various possible definitions of genera are equivalent.

PROOF. Let $G=\{1,\sigma,\sigma^2,\dots,\sigma^{n-1}\}$ be the Galois group, and define a function $F:\mathbb{Z}\to K^\times$ by $F(0)=1$ and

$$F(k)=x\sigma(x)\sigma^2(x)\cdots\sigma^{k-1}(x)\qquad\text{for } k\geq 1.$$

Then we have

$$\begin{aligned}F(k+l)&=x\sigma(x)\sigma^2(x)\cdots\sigma^{k+l-1}(x)\\&=\big(x\sigma(x)\sigma^2(x)\cdots\sigma^{k-1}(x)\big)\sigma^k\big(x\sigma(x)\sigma^2(x)\cdots\sigma^{l-1}(x)\big)\\&=F(k)\sigma^k(F(l)),\end{aligned}\tag{$*$}$$

The condition that $N_{K/F}(x)=1$ is exactly the condition that $F(n)=1$. Then $F(k+n)=F(k)\sigma^n(F(1))=F(k)$ for all k, and it is meaningful to define a 1-cochain $f:G\to K^\times$ in $C^1(G,K^\times)$ by $f(\sigma^k)=F(k)$. Condition $(*)$ implies that $f(\sigma^k\sigma^l)=f(\sigma^k)\sigma^k(f(\sigma^l))$, and hence f is a cocycle in $Z^1(G,K^\times)$. Theorem 3.17 shows that f is a coboundary in $B^1(G,K^\times)$, necessarily satisfying $f(\tau)=\tau(y)y^{-1}$ for some $y\in K^\times$ and all $\tau\in G$. Taking $\tau=\sigma$, we obtain $x=f(\sigma)=\sigma(y)y^{-1}$, as required. □

Our final result concerning $H^q(\mathrm{Gal}(K/F), K^\times)$ for this chapter gives further information about the special case in which $\mathrm{Gal}(K/F)$ is cyclic, but now for general q. In combination with the study of crossed-product algebras, the case $q = 2$ of this result provides a way of constructing new examples of noncommutative division algebras. A key step in the proof makes use of a fundamental general property concerning cohomology of groups, and we therefore digress in Section 5 to establish this property.

5. Digression on Cohomology of Groups

This section develops general material about cohomology of groups. Although the earlier sections of this chapter are helpful for motivation, the results that we discuss in this section do not rely on any previous material in this volume. It will be assumed that the reader is familiar with the definitions of complexes and exact sequences in Chapter X of *Basic Algebra*, as well as with the application of tensor-product functors and Hom functors to exact sequences and complexes. The material in Chapter VII of *Basic Algebra* on cohomology of groups will be helpful as background, but it is unnecessary from a logical point of view. If R is a ring with identity, we denote by $\mathcal{C}_R$ the category of all unital left R modules.

Let G be a group, not necessarily finite. We shall work with the integral group ring $\mathbb{Z}G$ of G. It has the universal mapping property that whenever G acts by automorphisms on an abelian group M, then the action by G on M extends to $\mathbb{Z}G$ in a unique way that makes M into a unital left $\mathbb{Z}G$ module.

Here is a brief overview of what is to happen in this section: If G acts on the abelian group M by automorphisms, then the abelian group $C^n(G, M)$ of n-cochains is the set of functions into M from the n-fold product of G with itself, the operation being given by addition of the values of the functions. To define the cohomology group $H^n(G, M)$, one introduces suitable homomorphisms known as "coboundary maps" $\delta_n : C^n(G, M) \to C^{n+1}(G, M)$ and shows that the sequence

$$0 \longrightarrow C_0(G, M) \xrightarrow{\delta_0} \cdots \xrightarrow{\delta_{n-1}} C_n(G, M) \xrightarrow{\delta_n} C_{n+1}(G, M) \longrightarrow \cdots$$

of abelian groups and homomorphisms is a complex in the category $\mathcal{C}_\mathbb{Z}$. Then it is meaningful to define $H^n(G, M) = (\ker \delta_n)/(\mathrm{image}\, \delta_{n-1})$ for $n \geq 0$ if we adopt the convention that $\mathrm{image}\, \delta_{-1} = 0$. The first thing that we shall do in this section is to exhibit a certain exact sequence in the category $\mathcal{C}_{\mathbb{Z}G}$ such that the above complex is obtained from it by application of the functor $\mathrm{Hom}_{\mathbb{Z}G}(\,\cdot\,, M)$ and the dropping of one term of the form $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M)$. Except for a single term $\mathbb{Z}$, the members of this exact sequence will all be free $\mathbb{Z}G$ modules, and the exact sequence will be called the "standard resolution of $\mathbb{Z}$ in the category $\mathcal{C}_{\mathbb{Z}G}$." The exactness is proved in Theorem 3.20, and the application of $\operatorname{Hom}_{\mathbb{Z}G}(\,\cdot\,, M)$ to it appears after the proof of the theorem.

The next thing that we shall do is show that if the standard resolution of $\mathbb{Z}$ is changed to any exact sequence in $\mathcal{C}_{\mathbb{Z}G}$ in such a way that the free $\mathbb{Z}G$ modules are replaced by other free $\mathbb{Z}G$ modules and the module $\mathbb{Z}$ is left unchanged, then application of $\operatorname{Hom}_{\mathbb{Z}G}(\,\cdot\,, M)$ to the new exact sequence leads to canonically isomorphic cohomology groups. This result appears below as Theorem 3.31. In brief, the cohomology groups $H^n(G, M)$ can be computed starting from any "free resolution of $\mathbb{Z}$" in the category $\mathcal{C}_{\mathbb{Z}G}$ in place of the standard resolution.

We begin by constructing the "standard resolution of $\mathbb{Z}$." For $n \geq 0$, let F_n be the free abelian group with $\mathbb{Z}$ basis the set of all $(n{+}1)$-tuples $(g_0, \dots, g_n)$ with all $g_j \in G$. The group G acts on F_n by automorphisms, the action on the members of the $\mathbb{Z}$ basis being

$$g(g_0, \dots, g_n) = (gg_0, \dots, gg_n).$$

The universal mapping property of $\mathbb{Z}G$ then allows us to regard each F_n as a unital left $\mathbb{Z}G$ module.

Lemma 3.19. For $n \geq 0$, the left $\mathbb{Z}G$ module F_n is a free $\mathbb{Z}G$ module with $\mathbb{Z}G$ basis consisting of all $(n{+}1)$-tuples $(1, g_1, \dots, g_n)$, i.e., all $\mathbb{Z}$ basis elements with $g_0 = 1$.

Proof. The formula $g_0(1, g_0^{-1}g_1, \dots, g_0^{-1}g_n) = (g_0, g_1, \dots, g_n)$ shows that all members of the $\mathbb{Z}$ basis defining F_n are $\mathbb{Z}G$ images of the asserted $\mathbb{Z}G$ basis; hence the asserted $\mathbb{Z}G$ basis is a spanning set of F_n relative to $\mathbb{Z}G$. Suppose that there are finitely many distinct members h_j of G and finitely many distinct $(n{+}1)$-tuples $(1, g_{i,1}, \dots, g_{i,n})$, and members $\sum_j n_{ij}h_j$ of $\mathbb{Z}G$ such that

$$\sum_i \Big(\sum_j n_{ij}h_j\Big)(1, g_{i,1}, \dots, g_{i,n}) = 0.$$

Then
$$\sum_{i,j} n_{ij}(h_j, h_jg_{i,1}, \dots, h_jg_{i,n}) = 0.$$

Since the h_j's are distinct as j varies and the n-tuples $(g_{i,1}, \dots, g_{i,n})$ are distinct as i varies, the $(n{+}1)$-tuples $(h_j, h_jg_{i,1}, \dots, h_jg_{i,n})$ are distinct as the pair (i, j) varies. Thus the $\mathbb{Z}$ independence implies that $n_{ij} = 0$ for all i and j. This proves the lemma. $\square$

For $n \geq 1$, we define $\partial_{n-1} : F_n \to F_{n-1}$ as a function from the $\mathbb{Z}$ basis into F_{n-1} by

$$\partial_{n-1}(g_0, \dots, g_n) = \sum_{i=0}^{n} (-1)^i (g_0, \dots, \widehat{g_i}, \dots, g_n),$$

where the symbol $\widehat{\ }$ indicates an expression to be omitted. We extend ∂_{n-1} to all of F_n by the universal mapping property of free abelian groups. For g in G and for any $\mathbb{Z}$ generator x of F_n, it is evident that $\partial_{n-1}(gx) = g(\partial_{n-1}(x))$. Since ∂_{n-1} is a homomorphism of abelian groups, the formula $\partial_{n-1}(gx) = g(\partial_{n-1}(x))$ extends to all x's in F_n. Since G and $\mathbb{Z}$ generate $\mathbb{Z}G$, we obtain $\partial_{n-1}(rx) = r(\partial_{n-1}(x))$ for all $r \in \mathbb{Z}G$ and all $x \in F_n$. In other words, each ∂_{n-1} is a $\mathbb{Z}G$ homomorphism.

We shall make use of one additional $\mathbb{Z}G$ homomorphism. According to Lemma 3.19, the $\mathbb{Z}G$ module F_0 is free on the $\mathbb{Z}G$ basis $\{(1)\}$. Let us think of the group G as acting trivially by automorphisms on the abelian group $\mathbb{Z}$. Under this action, $\mathbb{Z}$ becomes a $\mathbb{Z}G$ module. Define $\varepsilon : F_0 \to \mathbb{Z}$ to be the $\mathbb{Z}G$ homomorphism with $\varepsilon((1)) = 1$. Then $\varepsilon((g_0)) = g_0(\varepsilon((1)) = g_0 \cdot 1 = 1$ for all $g_0 \in G$. The $\mathbb{Z}G$ homomorphism ε is called the **augmentation map**.

Theorem 3.20. If G is any group, then the sequence

$$\cdots \xrightarrow{\partial_{n+1}} F_{n+1} \xrightarrow{\partial_n} F_n \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_0} F_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

of left unital $\mathbb{Z}G$ modules and $\mathbb{Z}G$ homomorphisms is exact.

REMARKS. The displayed sequence is called the **standard resolution of** $\mathbb{Z}$ in the category $\mathcal{C}_{\mathbb{Z}G}$. The proof will be preceded by two lemmas.

Lemma 3.21. The sequence

$$\cdots \xrightarrow{\partial_{n+1}} F_{n+1} \xrightarrow{\partial_n} F_n \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_0} F_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

in $\mathcal{C}_{\mathbb{Z}G}$ is a complex, i.e., $\partial_{n-1}\partial_n = 0$ for $n \geq 1$ and also $\varepsilon\partial_0 = 0$.

PROOF. With the understanding that the symbol $\widehat{\ }$ indicates an expression to be omitted, we have

$$\begin{aligned}\partial_{n-1}\partial_n(g_0,\dots,g_n) &= \sum_{i=0}^{n}(-1)^i\partial_{n-1}(g_0,\dots,\widehat{g_i},\dots,g_n)\\ &= \sum_{i=0}^{n}(-1)^i\sum_{j=0}^{i-1}(-1)^j(g_0,\dots,\widehat{g_j},\dots,\widehat{g_i},\dots,g_n)\\ &\quad+\sum_{i=0}^{n}(-1)^i\sum_{j=i+1}^{n}(-1)^{j+1}(g_0,\dots,\widehat{g_i},\dots,\widehat{g_j},\dots,g_n)\\ &= \sum_{i=0}^{n}\sum_{j=0}^{i-1}(-1)^{i+j}(g_0,\dots,\widehat{g_j},\dots,\widehat{g_i},\dots,g_n)\\ &\quad-\sum_{i=0}^{n}\sum_{j=i+1}^{n}(-1)^{i+j}(g_0,\dots,\widehat{g_i},\dots,\widehat{g_j},\dots,g_n).\end{aligned}$$

If we interchange the order of summation in the second double sum on the right, we see that the result equals the first double sum on the right. Thus the difference is 0.

This handles all the consecutive compositions except for $\varepsilon\partial_0$. For this we have $\varepsilon\partial_0(g_0, g_1) = \varepsilon(g_1) - \varepsilon(g_0) = 1 - 1 = 0$. □

Lemma 3.22. Fix s in G. For $n \geq 0$, define a homomorphism $h_n : F_n \to F_{n+1}$ of abelian groups to be the additive extension of the function with

$$h_n(g_0,\dots,g_n) = (s, g_0,\dots,g_n),$$

and define $h_{-1} : \mathbb{Z} \to F_0$ by $h_{-1}(k) = k(s)$. Then $\partial_n h_n + h_{n-1}\partial_{n-1} = 1$ for $n \geq 1$, and also $\partial_0 h_0 + h_{-1}\varepsilon = 1$.

PROOF. On the $\mathbb{Z}$ basis of $(n+1)$-tuples in F_n, we have

$$\begin{aligned}\partial_n h_n(g_0,\dots,g_n) &= \partial_n(s, g_0,\dots,g_n)\\ &= (g_0,\dots,g_n) + \sum_{i=0}^{n}(-1)^{i+1}(s, g_0,\dots,\widehat{g_i},\dots,g_n)\end{aligned}$$

and also

$$h_{n-1}\partial_{n-1}(g_0,\dots,g_n) = \sum_{i=0}^{n}(-1)^i(s, g_0,\dots,\widehat{g_i},\dots,g_n).$$

The sum of these is $(g_0,\dots,g_n)$, as required. Also,

$$\partial_0 h_0(g_0) = \partial_0(s, g_0) = (g_0) - (s) \qquad\text{and}\qquad h_{-1}\varepsilon(g_0) = h_{-1}1 = (s).$$

Thus $\partial_0 h_0(g_0) + h_{-1}\varepsilon(g_0) = (g_0)$, and $\partial_0 h_0 + h_{-1}\varepsilon = 1$. □

PROOF OF THEOREM 3.20. Lemma 3.21 gives $\operatorname{image} \partial_n \subseteq \ker \partial_{n-1}$ and $\operatorname{image} \partial_0 \subseteq \ker \varepsilon$. For the reverse of the first inclusion, let $x \in F_n$ be given with $\partial_{n-1}x = 0$ and $n \geq 1$. Then Lemma 3.22 gives $x = \partial_n h_n x + h_{n-1}\partial_{n-1}x$. The second term on the right side is 0, and therefore $x = \partial_n(h_n x)$ is in $\operatorname{image} \partial_n$.

For the reverse of the inclusion $\operatorname{image} \partial_0 \subseteq \ker \varepsilon$, let $x \in F_0$ be given with $\varepsilon x = 0$. Then Lemma 3.22 gives $x = \partial_0 h_0 x + h_{-1}\varepsilon x$. The second term on the right side is 0, and therefore $x = \partial_0(h_0 x)$ is in $\operatorname{image} \partial_0$. □

With the standard resolution of $\mathbb{Z}$ in $\mathcal{C}_{\mathbb{Z}G}$ now known to be exact, we examine the effect of applying the functor $\operatorname{Hom}_{\mathbb{Z}G}(\,\cdot\,, M)$ to it. This functor is contravariant and carries $\mathcal{C}_{\mathbb{Z}G}$ to the category $\mathcal{C}_{\mathbb{Z}}$ of all abelian groups. On a unital left $\mathbb{Z}G$ module F, this functor yields the abelian group $\operatorname{Hom}_{\mathbb{Z}G}(F, M)$. On a $\mathbb{Z}$ module homomorphism $\varphi : F \to F'$, it yields the homomorphism

$$\operatorname{Hom}(\varphi, 1) : \operatorname{Hom}_{\mathbb{Z}G}(F', M) \to \operatorname{Hom}_{\mathbb{Z}G}(F, M)$$

of abelian groups given by $\operatorname{Hom}(\varphi, 1)(\psi) = \psi \circ \varphi$ for $\psi \in \operatorname{Hom}_{\mathbb{Z}G}(F', M)$. We know from Chapter X of *Basic Algebra* that this functor carries complexes to complexes but does not necessarily preserve exactness.

Before applying $\operatorname{Hom}_{\mathbb{Z}G}(\,\cdot\,, M)$ to the standard resolution of $\mathbb{Z}$, it is customary to drop the term $\mathbb{Z}$ and the augmentation map, obtaining a modified sequence

$$\cdots \xrightarrow{\partial_{n+1}} F_{n+1} \xrightarrow{\partial_n} F_n \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_0} F_0 \longrightarrow 0$$

that is still a complex in $\mathcal{C}_{\mathbb{Z}G}$. Let us define $d_n = \operatorname{Hom}(\partial_n, 1)$. Then the result of applying $\operatorname{Hom}_{\mathbb{Z}G}(\,\cdot\,, M)$ to the modified complex is the complex

$$0 \longrightarrow \operatorname{Hom}_{\mathbb{Z}G}(F_0, M) \xrightarrow{d_0} \cdots \operatorname{Hom}_{\mathbb{Z}G}(F_n, M) \xrightarrow{d_n} \operatorname{Hom}_{\mathbb{Z}G}(F_{n+1}, M) \xrightarrow{d_{n+1}}$$

in $\mathcal{C}_{\mathbb{Z}}$. To each φ in $\operatorname{Hom}_{\mathbb{Z}G}(F_n, M)$, we associate $f = \Phi(\varphi)$ in $C^n(G, M)$ by the definition

$$f(g_1, \ldots, g_n) = \varphi(1, g_1, g_1g_2, \ldots, g_1 \cdots g_n).$$

Any member φ of $\operatorname{Hom}_{\mathbb{Z}G}(F_n, M)$ is determined by its values on $(n+1)$-tuples $(1, g_1, \ldots, g_n)$, since we can factor out the first entry of the argument of φ and commute it past φ, and it follows that the system of group homomorphisms

$$\Phi_n : \operatorname{Hom}_{\mathbb{Z}G}(F_n, M) \to C^n(G, M)$$

is a system of isomorphisms of abelian groups. Let

$$\delta_n : C^n(G, M) \to C^{n+1}(G, M)$$

be the map corresponding to $d_n : \operatorname{Hom}_G(F_n, M) \to \operatorname{Hom}_G(F_{n+1}, M)$ under this system of isomorphisms, namely $\delta_n = \Phi_{n+1} \circ d_n \circ \Phi_n^{-1}$. We can calculate δ_n explicitly as follows: If $f = \Phi_n(\varphi)$, then $\delta_n f = (\Phi_{n+1} d_n \Phi_n^{-1})(\Phi_n)(\varphi) = \Phi_{n+1} d_n \varphi$, and therefore

$$\begin{aligned}
(\delta_n f)(g_1, \dots, g_{n+1}) &= (d_n\varphi)(1, g_1, g_1g_2, \dots, g_1 \cdots g_{n+1}) \\
&= \varphi(\partial_n(1, g_1, g_1g_2, \dots, g_1 \cdots g_{n+1})) \\
&= \varphi(g_1, g_1g_2, \dots, g_1 \cdots g_{n+1}) \\
&\quad + \sum_{i=1}^{n} (-1)^i \varphi(1, g_1, \dots, \widehat{g_1 \cdots g_i}, \dots, g_1 \cdots g_{n+1}) \\
&\quad + (-1)^{n+1} \varphi(1, g_1, \dots, g_1 \cdots g_n) \\
&= g_1(f(g_2, g_3, \dots, g_{n+1})) \\
&\quad + \sum_{i=1}^{n} (-1)^i f(g_1, \dots, \widehat{g_i}, \dots, g_{n+1}) \\
&\quad + (-1)^{n+1} f(g_1, \dots, g_n).
\end{aligned}$$

Comparing this formula with the original formula defining δ_n in Chapter VII of *Basic Algebra*, we get a match. That is, we have obtained the complex in $\mathcal{C}_{\mathbb{Z}}$ defining the usual groups $H^n(G, M)$ by applying $\operatorname{Hom}_{\mathbb{Z}G}(\,\cdot\,, M)$ to the standard resolution of $\mathbb{Z}$ in $\mathcal{C}_{\mathbb{Z}G}$ and implementing the system of isomorphisms Φ_n. In particular, we obtain a more conceptual proof than in *Basic Algebra* of the fact that the sequence

$$0 \longrightarrow C_0(G, M) \xrightarrow{\delta_0} \cdots \xrightarrow{\delta_{n-1}} C_n(G, M) \xrightarrow{\delta_n} C_{n+1}(G, M) \longrightarrow \cdots$$

is a complex and that cohomology groups are therefore well defined.

This completes the discussion of the first main point of the section as outlined in the overview at the beginning. Next, any exact sequence

$$\cdots \xrightarrow{\partial'_{n+1}} F'_{n+1} \xrightarrow{\partial'_n} F'_n \xrightarrow{\partial'_{n-1}} \cdots \xrightarrow{\partial'_0} F'_0 \xrightarrow{\varepsilon'} \mathbb{Z} \longrightarrow 0$$

in the category $\mathcal{C}_{\mathbb{Z}G}$ in which all $\mathbb{Z}G$ modules F'_n for $n \geq 0$ are free $\mathbb{Z}G$ modules is called a **free resolution of** $\mathbb{Z}$ in the category $\mathcal{C}_{\mathbb{Z}G}$. The second main point of the section is that if we apply the functor $\operatorname{Hom}_{\mathbb{Z}G}(\,\cdot\,, M)$ to this sequence with $\mathbb{Z}$ dropped, then the consecutive quotients of kernels modulo images are canonically isomorphic to the cohomology groups $H^n(G, M)$ obtained above. Thus $H^n(G, M)$ can be computed from *any* free resolution of $\mathbb{Z}$, and we are not obliged to use the standard free resolution. This result is stated precisely as Theorem 3.31 below.

By way of preparation, let us establish a slightly more general setting and work with it for a moment. Let $\mathcal{C}_R$ be the category of all unital left R modules, where R is any ring with identity. According to circumstances, a complex X in $\mathcal{C}_R$ might be written with decreasing indices as

$$X : \qquad \cdots \xrightarrow{\partial_{n+1}} X_{n+1} \xrightarrow{\partial_n} X_n \xrightarrow{\partial_{n-1}} X_{n-1} \xrightarrow{\partial_{n-2}} \cdots$$

or with increasing indices as

$$X : \qquad \cdots \xrightarrow{d_{n-2}} X_{n-1} \xrightarrow{d_{n-1}} X_n \xrightarrow{d_n} X_{n+1} \xrightarrow{d_{n+1}} \cdots .$$

Mathematically these complexes amount to the same thing: if we rename each X_k in the second complex as X_{-k} and rename each d_k as ∂_{-k-1}, then we obtain the first complex. However, it is convenient to allow both systems of indexing because of applications.

For the first complex, which has decreasing indices, we define the n^{th} **homology** of X, written $H_n(X)$, by

$$H_n(X) = (\ker \partial_{n-1})/(\text{image}\, \partial_n).$$

For the second complex, which has increasing indices, we define the n^{th} **cohomology** of X, written $H^n(X)$, by

$$H^n(X) = (\ker d_n)/(\text{image}\, d_{n-1}).$$

In both cases the integer n is called the **degree**. In either case the homology or cohomology is again a module in $\mathcal{C}_R$. The condition that X be a complex is equivalent to the condition that the image of each incoming map be contained in the kernel of the corresponding outgoing map, and this is precisely the condition that the homology or cohomology be meaningful. Exactness at a particular module in one of the complexes is the statement that the image of the incoming map equals the kernel of the outgoing map. Thus the homology or cohomology of X measures the extent to which the complex X fails to be exact.

Because the nature of the indexing of a complex is not mathematically significant, we will treat only the case of increasing indices for a while, and the modules associated to our complexes will therefore be cohomology modules. A

cochain map[2] between two complexes X and Y in the same category $\mathcal{C}_R$ is a system $f = \{f_n\}$ of R homomorphisms $f_n : X_n \to Y_n$ such that the various squares commute in Figure 3.1.

$$\begin{tikzcd}
X : & \cdots \arrow[r, "d_{n-2}"] & X_{n-1} \arrow[r, "d_{n-1}"] \arrow[d, "f_{n-1}"] & X_n \arrow[r, "d_n"] \arrow[d, "f_n"] & X_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, "f_{n+1}"] & \cdots \\
Y : & \cdots \arrow[r, "d'_{n-2}"] & Y_{n-1} \arrow[r, "d'_{n-1}"] & Y_n \arrow[r, "d'_n"] & Y_{n+1} \arrow[r, "d'_{n+1}"] & \cdots
\end{tikzcd}$$

FIGURE 3.1. A cochain map $f : X \to Y$.

Proposition 3.23. A cochain map $f : X \to Y$ as in Figure 3.1 induces an R homomorphism on cohomology $H^n(X) \to H^n(Y)$ in each degree.

PROOF. Suppose that x_n is in $\ker d_n$, i.e., that $d_n(x_n) = 0$. The commutativity of the right square gives $d'_n(f_n(x_n)) = f_{n+1}(d_n(x_n)) = 0$, and hence $f_n(x_n)$ is in $\ker d'_n$. Suppose that x_n is in $\operatorname{image} d_{n-1}$, i.e., that $x_n = d_{n-1}(x_{n-1})$ for some x_{n-1}. The commutativity of the left square gives $f_n(x_n) = f_n d_{n-1}(x_{n-1}) = d'_{n-1}(f_{n-1}(x_{n-1}))$, and hence $f_n(x_n)$ is in image d'_{n-1}. Then it follows that $f_n\big|_{\ker d_n}$ descends to the quotient $(\ker d_n)/(\operatorname{image} d_{n-1})$, yielding a map of $H^n(X)$ into $H^n(Y)$. □

Suppose in the situation of Figure 3.1 that $g = \{g_n\}$ is a second cochain map of X into Y. We say that f is **homotopic**[3] to g, written $f \simeq g$, if there is a system $h = \{h_n\}$ of maps $h_n : X_n \to Y_{n-1}$ in $\mathcal{C}_R$ such that $d'h + hd = f - g$, i.e., if $d'_{n-1}h_n + h_{n+1}d_n = f_n - g_n$ for all n.

Proposition 3.24. In the situation of Figure 3.1 if $f = \{f_n\}$ and $g = \{g_n\}$ are two cochain maps of X into Y and if f and g are homotopic, then f and g induce *identical* maps $H^n(X) \to H^n(Y)$ in each degree.

PROOF. Suppose that $d_n(x_n) = 0$. Then $f_n(x_n) - g_n(x_n) = d'_{n-1}(h_n(x_n)) + h_{n+1}(d_n(x_n)) = d'_{n-1}(h_n(x_n)) + 0$ shows that the images of x_n under f_n and g_n in Y_n differ by a member of image d'_{n-1}. □

Now we bring free R modules into the discussion.

[2] The analogous kind of system in which the complexes have decreasing indices is called a **chain map**.

[3] An analogous definition is to be made in the case of two chain maps. If the maps of X are $\partial_n : X_{n+1} \to X_n$ and the maps of Y are $\partial'_n : Y_{n+1} \to Y_n$, then we are to have $h_n : X_n \to Y_{n+1}$ with $\partial'_n h_n + h_{n-1}\partial_{n-1} = f_n - g_n$.

Proposition 3.25. For the diagram

$$\begin{tikzcd}
F \arrow[r, "\partial"] \arrow[d, dashed, "\widetilde{f}"] & M \arrow[r, "\partial_1"] \arrow[d, "f"] & N \arrow[d, "f_1"] \\
F' \arrow[r, "\partial'"] & M' \arrow[r, "\partial'_1"] & N'
\end{tikzcd}$$

in $\mathcal{C}_R$, suppose that the top and bottom rows are exact at M and M', suppose that the square on the right commutes, and suppose that F is a free R module. Then there exists an R homomorphism $\widetilde{f} : F \to F'$ that makes the left square commute.

PROOF. If x is a free generator of F, then $0 = f_1\partial_1\partial(x) = \partial'_1(f\partial x)$. By exactness at M', $f\partial x$ lies in image(∂'). Choose any $y \in F'$ with $\partial' y = f\partial x$, and define $\widetilde{f}(x)$ to be this y. Then $f\partial x = \partial'\widetilde{f}x$, and the left square commutes at x. The universal mapping property of free R modules says that $\widetilde{f}$ extends to an R homomorphism of F into F', and the extension has $f\partial = \partial'\widetilde{f}$, as required. □

Corollary 3.26. In the category $\mathcal{C}_{\mathbb{Z}G}$, if the rows of the diagram

$$\begin{tikzcd}
{} \arrow[r, "\partial'_{n+1}"] & X_{n+1} \arrow[r, "\partial'_n"] \arrow[d, "f_{n+1}"] & X_n \arrow[r, "\partial'_{n-1}"] \arrow[d, "f_n"] & \cdots \arrow[r, "\partial'_0"] & X_0 \arrow[r, "\varepsilon'"] \arrow[d, "f_0"] & \mathbb{Z} \arrow[r] \arrow[d, "1"] & 0 \\
{} \arrow[r, "\partial''_{n+1}"] & Y_{n+1} \arrow[r, "\partial''_n"] & Y_n \arrow[r, "\partial''_{n-1}"] & \cdots \arrow[r, "\partial''_0"] & Y_0 \arrow[r, "\varepsilon'"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

are free resolutions and the vertical identity map $1 : \mathbb{Z} \to \mathbb{Z}$ is given, then the remaining vertical maps,

$$f_0 : X_0 \to Y_0, \quad \dots, \quad f_n : X_n \to Y_n, \quad f_{n+1} : X_{n+1} \to Y_{n+1}, \quad \dots,$$

can be constructed inductively from the right to make all the squares commute.

REMARK. The resulting system $f = \{f_n\}$ is called a **chain map over** the identity map $1 : \mathbb{Z} \to \mathbb{Z}$.

PROOF. There is no harm in including a vertical 0 map at the right between the two 0 modules. Certainly the square whose verticals are the identity map $1 : \mathbb{Z} \to \mathbb{Z}$ and the 0 map commutes. Proposition 3.25 is to be applied first to this square and the second square from the right (with vertical f_0 to be constructed and vertical $1 : \mathbb{Z} \to \mathbb{Z}$ given) to construct f_0, then to the second and third squares from the right to construct f_1, and so on, inductively. □

Proposition 3.27. For the diagram

$$\begin{tikzcd}
\widetilde{F} \arrow[r, "\partial"] \arrow[d, "\widetilde{f}"] & F \arrow[r, "\partial_1"] \arrow[d, "f"] \arrow[dl, dashed, "h"] & N \arrow[d, "f_1"] \arrow[dl, "h_1"] \\
\widetilde{F} \arrow[r, "\partial"'] & F \arrow[r, "\partial_1"'] & N
\end{tikzcd}$$

in $\mathcal{C}_R$, suppose that the top and bottom rows are exact at F, that the left and right squares commute, that $\widetilde{F}$ and F are free R modules, and that $h_1 : N \to F$ exists with $f_1 - \partial_1 h_1$ vanishing on image(∂_1). Then there exists $h : F \to \widetilde{F}$ such that $\partial h + h_1 \partial_1 = f$, and this property implies that $f - \partial h$ vanishes on image(∂).

PROOF. If x is a free generator of F, then $f(x) - h_1(\partial_1(x))$ is in $\ker(\partial_1)$ because $\partial_1(fx - h_1\partial_1 x) = f_1\partial_1 x - \partial_1 h_1 \partial_1 x = (f_1 - \partial_1 h_1)(\partial_1 x)$ and because $f_1 - \partial_1 h_1$ vanishes on image(∂_1) by assumption. Therefore $f(x) - h_1(\partial_1(x))$ is in image(∂), and we can write $f(x) - h_1(\partial_1(x)) = \partial a$ for some $a \in \widetilde{F}$. Put $h(x) = a$. Then $\partial h x = \partial a = fx - h_1 \partial_1 x$, and h has the required property on the generator x. The universal mapping property of the free R module F allows us to extend h to an R homomorphism $h : F \to \widetilde{F}$, and the extension satisfies $\partial h = f - h_1 \partial_1$. Once h has this property, then necessarily $(f - \partial h)\partial = (h_1\partial_1)\partial = h_1(\partial_1\partial) = 0$. □

Corollary 3.28. In the category $\mathcal{C}_{\mathbb{Z}G}$, if a free resolution $X = \{X_n\}$ of $\mathbb{Z}$ and a chain map $f = \{f_n\}$ of X with itself are given such that the map from $\mathbb{Z}$ to itself is 0, then the chain map f is homotopic to the zero chain map $g = \{g_n\}$ with $g_n = 0$ for all n.

PROOF. We are given the diagram

$$\begin{tikzcd}
{} \arrow[r] & X_n \arrow[r] \arrow[d, "f_n"] & \cdots \arrow[r, "\partial'_1"] & X_1 \arrow[r, "\partial'_0"] \arrow[d, "f_1"] \arrow[dl, dashed, "h_1"] & X_0 \arrow[r, "\varepsilon'"] \arrow[d, "f_0"] \arrow[dl, dashed, "h_0"] & \mathbb{Z} \arrow[r] \arrow[d, "0"] \arrow[dl, "h_{-1}"] & 0 \\
{} \arrow[r] & X_n \arrow[r] & \cdots \arrow[r, "\partial'_1"] & X_1 \arrow[r, "\partial'_0"] & X_0 \arrow[r, "\varepsilon'"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

in the category $\mathcal{C}_{\mathbb{Z}G}$ with the two rows as free resolutions and all squares commuting. We are to construct maps $h_n : X_n \to X_{n+1}$ with $\partial'_n h_n + h_{n-1}\partial'_{n-1} = f_n$. Let h_{-2} be the 0 map from the top 0 module to the bottom $\mathbb{Z}$, and let h_{-1} be the 0 map from the top $\mathbb{Z}$ to the bottom X_0. Then $\partial'_n h_n + h_{n-1}\partial'_{n-1} = f_n$ is satisfied for $n = -1$ because the map f_{-1} is the 0 map from $\mathbb{Z}$ to itself. Proposition 3.27 then allows us to construct inductively first h_0, then h_1, then h_2, and so on. □

Corollary 3.29. In the category $\mathcal{C}_{\mathbb{Z}G}$, if a free resolution $X = \{X_n\}$ of $\mathbb{Z}$ and a chain map $f = \{f_n\}$ of X with itself are given such that the map from $\mathbb{Z}$ to itself is the identity 1, then the chain map f is homotopic to the identity chain map $g = \{g_n\}$ with $g_n = 1$ for all n.

PROOF. Apply Corollary 3.28 to $f - 1$. □

Corollary 3.30. In the category $\mathcal{C}_{\mathbb{Z}G}$, if two free resolutions $X = \{X_n\}$ of $\mathbb{Z}$ and $Y = \{Y_n\}$ of $\mathbb{Z}$ are given and if two chain maps $f : X \to Y$ and $g : Y \to X$ are given such that the map from $\mathbb{Z}$ to itself in each case is the identity 1, then gf is homotopic to 1 and fg is homotopic to 1.

PROOF. Apply Corollary 3.29 to fg and then to gf. □

Theorem 3.31. If

$$\cdots \xrightarrow{\partial'_{n+1}} F'_{n+1} \xrightarrow{\partial'_n} F'_n \xrightarrow{\partial'_{n-1}} \cdots \xrightarrow{\partial'_0} F'_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

is any free resolution of $\mathbb{Z}$ in the category $\mathcal{C}_{\mathbb{Z}G}$ and M is a unital left $\mathbb{Z}G$ module, then $H^n(G, M)$ is canonically isomorphic to the n^{th} cohomology group of the complex in $\mathcal{C}_{\mathbb{Z}}$ given by

$$0 \longrightarrow \operatorname{Hom}_{\mathbb{Z}G}(F'_0, M) \xrightarrow{d_0} \cdots \operatorname{Hom}_{\mathbb{Z}G}(F'_n, M) \xrightarrow{d_n} \operatorname{Hom}_{\mathbb{Z}G}(F'_{n+1}, M) \xrightarrow{d_{n+1}}$$

with $d_n = \operatorname{Hom}(\partial'_n, 1)$ for $n \geq 0$.

PROOF. Let the resolution in the statement of the theorem be Y, and let X be the standard free resolution of $\mathbb{Z}$ in the category $\mathcal{C}_{\mathbb{Z}G}$. Two applications of Corollary 3.26 produce chain maps $f : X \to Y$ and $g : Y \to X$ over $1 : \mathbb{Z} \to \mathbb{Z}$. Corollary 3.30 shows that gf is homotopic to $1 = 1_X$ and fg is homotopic to $1 = 1_Y$. Apply the functor $\operatorname{Hom}_{\mathbb{Z}G}(\,\cdot\,, M)$ throughout, including to the members of the homotopies. Then we obtain chain maps

$$\operatorname{Hom}_{\mathbb{Z}G}(f, 1) : \operatorname{Hom}_{\mathbb{Z}G}(Y, M) \to \operatorname{Hom}_{\mathbb{Z}G}(X, M)$$

and

$$\operatorname{Hom}_{\mathbb{Z}G}(g, 1) : \operatorname{Hom}_{\mathbb{Z}G}(X, M) \to \operatorname{Hom}_{\mathbb{Z}G}(Y, M)$$

with

$$\operatorname{Hom}_{\mathbb{Z}G}(f, 1) \circ \operatorname{Hom}_{\mathbb{Z}G}(g, 1) \qquad \text{homotopic to } 1$$

and

$$\operatorname{Hom}_{\mathbb{Z}G}(g, 1) \circ \operatorname{Hom}_{\mathbb{Z}G}(f, 1) \qquad \text{homotopic to } 1.$$

Proposition 3.24 allows us to conclude that

$$\operatorname{Hom}_{\mathbb{Z}G}(f, 1) \circ \operatorname{Hom}_{\mathbb{Z}G}(g, 1) \text{ induces the identity on } H^*(\operatorname{Hom}_{\mathbb{Z}G}(X, M))$$

and

$$\operatorname{Hom}_{\mathbb{Z}G}(g, 1) \circ \operatorname{Hom}_{\mathbb{Z}G}(f, 1) \text{ induces the identity on } H^*(\operatorname{Hom}_{\mathbb{Z}G}(Y, M)).$$

Thus $\operatorname{Hom}_{\mathbb{Z}G}(g, 1)$ induces an isomorphism of each group $H^n(\operatorname{Hom}_{\mathbb{Z}G}(X, M))$ onto $H^n(\operatorname{Hom}_{\mathbb{Z}G}(Y, M))$. □

6. Relative Brauer Group when the Galois Group Is Cyclic

This section has two parts to it. The first part specializes Theorem 3.31 to compute group cohomology when the group in question is cyclic of finite order. The second part applies this computation to $H^2(\mathrm{Gal}(K/F), K^\times)$ and obtains information about Brauer groups. As a consequence we obtain new information about the classification of noncommutative division algebras.

Let G be a finite cyclic group of order n. Theorem 3.31 says that if G acts by automorphisms on an abelian group M, then $H^2(G, M)$ can be computed from any free resolution of $\mathbb{Z}$ in the category $\mathcal{C}_{\mathbb{Z}G}$. The standard resolution of $\mathbb{Z}$ is one such resolution. We shall construct another such resolution that is special to the case of G cyclic and that makes the cohomology more transparent.

Let $G = \{1, s, s^2, \dots, s^{n-1}\}$. Lemma 3.19 notes that the free abelian group on the 1-tuples $(1), (s), (s^2), \dots, (s^{n-1})$ is a free $\mathbb{Z}G$ module with $\mathbb{Z}G$ basis (1). In other words, the elements of the left $\mathbb{Z}G$ module $\mathbb{Z}G$ may be identified with the integer linear combinations of these 1-tuples. Define two operators T and N from the left $\mathbb{Z}G$ module $\mathbb{Z}G$ into itself by

$$\begin{aligned} T &= \text{multiplication by } (s) - (1), \\ N &= \text{multiplication by } (1) + (s) + \cdots + (s^{n-1}). \end{aligned}$$

Each of these respects addition and commutes with multiplication by (s), hence is a $\mathbb{Z}G$ module homomorphism. We shall compute the kernel and image of each.

The kernel of T consists of all elements for which left multiplication by (s) fixes the element. The elements of $\mathbb{Z}G$ are of the form $\sum_{j=0}^{n-1} c_j(s^j)$, and (s) times this gives $c_{n-1}(1) + \sum_{j=1}^{n-1} c_{j-1}(s^j)$. Since $(1), (s), \dots, (s^{n-1})$ form a $\mathbb{Z}$ basis, the condition to be in the kernel of T is that $c_{n-1} = c_0 = c_1 = \cdots = c_{n-2}$. Thus

$$\ker T = \big\{c\big((1) + (s) + \cdots + (s^{n-1})\big) \mid c \in \mathbb{Z}\big\}.$$

Also,

$$\begin{aligned} \text{image}\, T &= \{\text{integer polynomials in } (s) \text{ divisible by } (s) - (1)\} \\ &= \{\text{integer polynomials equal to 0 when } s \text{ is set equal to 1}\} \\ &= \Big\{\sum_{j=0}^{n-1} c_j(s^j) \;\Big|\; \sum_{j=0}^{n-1} c_j = 0\Big\}. \end{aligned}$$

In the case of the operator N, we have $N(s^j) = (1) + (s) + \cdots + (s^{n-1})$, and therefore $N\big(\sum_j c_j(s^j)\big) = \sum_j c_j\big((1) + (s) + \cdots + (s^{n-1})\big)$. Hence

$$\begin{aligned} \ker N &= \Big\{\sum_{j=0}^{n-1} c_j(s^j) \;\Big|\; \sum_{j=0}^{n-1} c_j = 0\Big\} = \text{image}\, T, \\ \text{image}\, N &= \big\{c\big((1) + (s) + \cdots + (s^{n-1})\big) \mid c \in \mathbb{Z}\big\} = \ker T. \end{aligned}$$

An immediate consequence of this and a supplementary argument concerning the augmentation map is the following proposition.

Proposition 3.32. If G is a finite cyclic group, then the sequence

$$\cdots \xrightarrow{T} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{T} \cdots \xrightarrow{T} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{T} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

is a free resolution of $\mathbb{Z}$ in the category $\mathcal{C}_{\mathbb{Z}G}$.

PROOF. We still need to check exactness at the first $\mathbb{Z}G$ from the right. The map ε is the $\mathbb{Z}G$ homomorphism with $\varepsilon((1)) = 1$. Hence $\varepsilon((s^j)) = 1$ for all j, and $\varepsilon\big(\sum_{j=0}^{n-1} c_j(s^j)\big) = \sum_{j=0}^{n-1} c_j$. Thus $\ker\varepsilon = \ker N = \operatorname{image} T$, and exactness is proved. □

Corollary 3.33. If G is a finite cyclic group and M is an abelian group on which G acts by automorphisms, then

$$H^2(G, M) \cong M^G\big/\big((1) + (s) + \cdots + (s^{n-1})\big)M,$$

where M^G is the subgroup of all elements of M fixed by G.

PROOF. Let us number the terms $\mathbb{Z}G$ in the resolution of Proposition 3.32 starting with index 0 from the right. Combining Proposition 3.32 with Theorem 3.31, we see that we may compute $H^2(G, M)$ as the cohomology of the complex obtained by applying the functor $\operatorname{Hom}_{\mathbb{Z}G}(\,\cdot\,, M)$ to the terms with indices 1, 2, 3 in the resolution in Proposition 3.32. Thus $H^2(G, M)$ is the cohomology at the middle of the complex

$$\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M) \xrightarrow{(\cdot)\circ N} \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M) \xrightarrow{(\cdot)\circ T} \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M).$$

The mapping $\alpha \mapsto \alpha((1))$ of $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M)$ into M is one-one and onto, and we can identify members α of $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M)$ with the corresponding elements $\alpha((1))$ accordingly. If α is in $\ker\big((\cdot)\circ T\big)$, then $\alpha(T((1))) = 0$, and we thus have $\alpha((s)) = \alpha((1))$ and $(s)\alpha((1)) = \alpha((1))$. Hence $\alpha((1))$ is in M^G. These steps can be reversed, and thus $\ker\big((\cdot)\circ T\big) = M^G$. If β is in $\operatorname{image}\big((\cdot)\circ N\big)$, then $\beta = \alpha \circ N$ for some $\alpha \in \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M)$, and thus

$$\beta((1)) = \alpha\big((1) + (s) + \cdots + (s^{n-1})\big) = \alpha((1)) + (s)\alpha((1)) + \cdots + (s^{n-1})\alpha((1)).$$

Since $\alpha((1))$ is a completely arbitrary element of M, we see that $\operatorname{image}\big((\cdot)\circ N\big) = \big((1) + (s) + \cdots + (s^{n-1})\big)M$, and the result follows. □

Now we specialize to the Galois case that has occupied our attention in this chapter. Let K/F be a finite Galois extension of fields. We are going to set $G = \operatorname{Gal}(K/F)$, $n = \dim_F K$, and $M = K^\times$. To take advantage of Corollary 3.33, we suppose that $\operatorname{Gal}(K/F)$ is cyclic. Then $M^G = (K^\times)^G = F^\times$. If x is an element of $K^\times$, then the orbit Gx is $\{x, sx, s^2x, \dots, s^{n-1}x\}$. Remembering that we are using additive notation in working with cohomology of groups and multiplicative notation in working with $K^\times$, we see that the element $\big((1) + (s) + \cdots + (s^{n-1})\big)$ of $\mathbb{Z}G$ is to be regarded as operating by giving the product of the members of an orbit in $K^\times$. This product for the orbit of $x \in K^\times$ is $N_{K/F}(x)$, and Corollary 3.33 thus specializes to the following result.

Corollary 3.34. If K/F is a finite Galois extension of fields such that $\operatorname{Gal}(K/F)$ is cyclic, then

$$H^2(\operatorname{Gal}(K/F), K^\times) \cong F^\times \big/ N_{K/F}(K^\times).$$

Corollary 3.34 considerably simplifies the proofs of Frobenius's Theorem about division algebras over the reals (Theorem 2.50) and Wedderburn's Theorem about finite division rings (Theorem 2.48), and thus the theory in Chapter III has added something to the theory of Chapter II even in these very special situations. In the case of the Frobenius theorem, the only nontrivial algebraic extension of $\mathbb{R}$ is $\mathbb{C}$, and thus Theorem 3.14 and Corollary 3.34 give

$$\begin{aligned} \mathcal{B}(\mathbb{R}) = \mathcal{B}(\mathbb{C}/\mathbb{R}) &\cong H^2(\operatorname{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{R}^\times) \\ &\cong \mathbb{R}^\times \big/ N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times) = \mathbb{R}^\times/(\mathbb{R}^\times)^+ \cong \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

Hence the reals and the quaternions are the only finite-dimensional central simple division algebras over $\mathbb{R}$.

In the case of the Wedderburn theorem, suppose that a finite field K splits a central division algebra over a field F with q elements. Say that $|K| = q^n$. For finite fields the Galois groups are always cyclic, and thus $\operatorname{Gal}(K/F)$ is cyclic of order n, generated by the map $x \mapsto x^q$. In view of Corollary 3.34, the Wedderburn theorem follows if $F^\times \big/ N_{K/F}(K^\times)$ is shown to be trivial, i.e., if the norm map $N_{K/F} : K^\times \to F^\times$ is onto. The group $K^\times$ is cyclic, say with a generator x_0 of order $q^n - 1$. Since the norm of an element is the product of the images under the Galois group, the norm of x_0 is given by

$$N_{K/F}(x_0) = x_0 x_0^q x_0^{q^2} \cdots x_0^{q^{n-1}} = x_0^{1+q+\cdots+q^{n-1}} = x_0^{\frac{q^n-1}{q-1}}.$$

This has order $q - 1$, not less, and thus is a generator of $F^\times$. Thus the norm map is onto $F^\times$.

For a more difficult example that we can settle completely, consider the case that $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{m}\,)$ for a square-free integer m other than 1. The Galois group in this case is a 2-element group and is in particular cyclic. Thus Corollary 3.34 applies. The norm of the member $x + y\sqrt{m}$ of K, where x and y are in $\mathbb{Q}$, is $x^2 - my^2$. The problem of determining the quotient group $F^\times \big/ N_{K/\mathbb{Q}}(K^\times)$ may be rephrased in terms of genera as in Section I.5. Specifically the field discriminant D is defined to be m if $m \equiv 1 \bmod 4$ and to be $4m$ if $m \not\equiv 1 \bmod 4$. A genus for $\mathbb{Q}(\sqrt{m}\,)$ is an equivalence class of primitive quadratic forms $ax^2 + bxy + cy^2$ whose discriminant matches the field discriminant D, except that the theory of Chapter I discards all negative definite forms. Equivalence is determined by the action of $\mathrm{SL}(2, \mathbb{Q})$. Lemma 1.13 shows for $D > 0$ that each nonzero rational number is a value taken on by the members of one and only one genus at points $(x, y) \neq (0, 0)$ with x and y both rational; for $D < 0$, Lemma 1.13 applies to positive definite forms and positive rational numbers. Let us now enlarge the definition of genera to include negative definite forms and negative rational numbers when $D < 0$.

The definition of the multiplication of classes of forms is set up so as to be compatible with multiplication of the values of the quadratic forms, and the genera define a group, the identity element being the principal genus. Since a representative of the principal genus is $x^2 - my^2$, the nonzero rational values corresponding to the principal genus are exactly the members of the group $N_{K/\mathbb{Q}}(K^\times)$. Consequently the quotient group $F^\times \big/ N_{K/\mathbb{Q}}(K^\times)$ is isomorphic to the group of genera.[4] The easy result concerning the group of genera is Theorem 1.14, which says that this group is finite abelian and that every nontrivial element has order 2; since $\mathcal{B}(K/F) \cong F^\times \big/ N_{K/\mathbb{Q}}(K^\times)$, Corollary 3.15 gives another way of seeing that every nontrivial element has order 2. The hard result, which appears in Problems 25–29 at the end of Chapter I, identifies the order of the group of genera explicitly.[5] If $D > 0$, then the order of the group of genera is $2^{g'}$, where $g' + 1$ is the number of distinct prime divisors of D; if $D < 0$, then the order of the group of genera is $2^{g'+1}$.

Consequently if m has $g + 1$ distinct prime divisors, then the relative Brauer group is a product of 2-element groups whose order is given by

$$\big|\mathcal{B}(\mathbb{Q}(\sqrt{m}\,)/\mathbb{Q})\big| = \begin{cases} 2^g & \text{if } m > 0 \text{ and } m \not\equiv 3 \bmod 4, \\ 2^{g+1} & \text{if } m > 0 \text{ and } m \equiv 3 \bmod 4, \\ 2^{g+1} & \text{if } m < 0 \text{ and } m \not\equiv 3 \bmod 4, \\ 2^{g+2} & \text{if } m < 0 \text{ and } m \equiv 3 \bmod 4. \end{cases}$$

[4] With the understanding that genera from negative definite forms are to be allowed if $D < 0$.

[5] In quoting this result, we are now making allowances for genera corresponding to negative definite forms.

The example with $K/\mathbb{Q}$ quadratic shows the kind of information that has to go into a complete determination of the relative Brauer group when $K/\mathbb{Q}$ is Galois. Showing that a relative Brauer group is nontrivial in a case with $\operatorname{Gal}(K/\mathbb{Q})$ cyclic is considerably easier. According to Corollary 3.34, all one needs to know is that the norm function does not carry $K^\times$ onto $\mathbb{Q}^\times$, and congruence conditions can be used as a first step in addressing this question; Problem 4 at the end of the chapter illustrates this principle. Problems 15–17 at the end of Chapter II give a construction in this situation of nontrivial central simple algebras over $\mathbb{Q}$ that are split by K, and such algebras whose dimension is the square of a prime are necessarily division algebras. Problems 6–12 at the end of the present chapter give a sufficient condition for obtaining a division algebra when the dimension is not the square of a prime.

7. Problems

1. Let A be a finite-dimensional central simple algebra over a field F, let K be a subfield of A, and let B be the centralizer of K in A.
   (a) Arguing as in the proof of Theorem 3.3, exhibit a one-one algebra homomorphism $A \otimes_F K \to \operatorname{End}_{B^o} A$.
   (b) Referring to the proof of Theorem 2.2 and counting dimensions with the aid of the Double Centralizer Theorem, prove that the mapping in (a) is onto $\operatorname{End}_{B^o} A$.
   (c) Deduce that $A \otimes_F K$ and B yield the same member of $\mathcal{B}(K)$.

2. Let $a = a(\sigma, \tau)$ be a 2-cocycle in $Z^2(\operatorname{Gal}(K/F), K^\times)$, where K/F is a finite Galois extension of fields. Prove for each τ that $\prod_{\sigma \in \operatorname{Gal}(K/F)} a(\sigma, \tau)$ lies in $F^\times$.

3. Let K/F be a finite Galois extension of fields with $\operatorname{Gal}(K/F)$ cyclic. Corollary 3.34 identifies $H^q(\operatorname{Gal}(K/F), K^\times)$ for $q = 2$. Identify this group for all other values of $q \geq 0$.

Problems 4–5 amplify the discussion of cyclic algebras that was begun in Problems 17–19 at the end of Chapter II. Problem 4 in effect produces an explicit division algebra of dimension 9 over $\mathbb{Q}$, and Problem 5 hints at the existence of an explicit division algebra of dimension n^2 over $\mathbb{Q}$ for each integer $n \geq 1$.

4. Let $\zeta = e^{2\pi i/7}$, and let $K = \mathbb{Q}(\zeta) \cap \mathbb{R}$.
   (a) Show that $K/\mathbb{Q}$ is a Galois extension of degree 3, that a basis for K over $\mathbb{Q}$ consists of $\tau_1 = \zeta + \zeta^{-1}$, $\tau_2 = \zeta^2 + \zeta^{-2}$, $\tau_3 = \zeta^3 + \zeta^{-3}$, and that the Galois group permutes τ_1, τ_2, τ_3 cyclically.
   (b) Show that if a, b, c are in $\mathbb{Q}$, then

$$\begin{aligned} N_{K/\mathbb{Q}}(a\tau_1 + b\tau_2 + c\tau_3) = abc(&\tau_1^3 + \tau_2^3 + \tau_3^3) \\ &+ (a^3 + b^3 + c^3 + 3abc)\tau_1\tau_2\tau_3 \\ &+ (a^2b + ac^2 + b^2c)(\tau_1^2\tau_2 + \tau_2^2\tau_3 + \tau_3^2\tau_1) \\ &+ (a^2c + ab^2 + bc^2)(\tau_1\tau_2^2 + \tau_2\tau_3^2 + \tau_3\tau_1^2). \end{aligned}$$

(c) Verify the following identities:

$$\tau_1 + \tau_2 + \tau_3 = -1,$$
$$\tau_1\tau_2 = \tau_1 + \tau_3, \quad \tau_1\tau_3 = \tau_2 + \tau_3, \quad \tau_2\tau_3 = \tau_1 + \tau_2,$$
$$\tau_1^2 = \tau_2 + 2, \quad \tau_2^2 = \tau_3 + 2, \quad \tau_3^2 = \tau_1 + 2.$$

(d) Combine (b) and (c) to show that

$$\begin{aligned} N_{K/\mathbb{Q}}(a\tau_1 + b\tau_2 + c\tau_3) = (a^3 &+ b^3 + c^3) - abc \\ &+ 3(a^2b + ac^2 + b^2c) - 4(a^2c + ab^2 + bc^2). \end{aligned}$$

(e) Under the assumption that a, b, c are integers with $\mathrm{GCD}(a, b, c) = 1$, show that $N_{K/\mathbb{Q}}(a\tau_1 + b\tau_2 + c\tau_3) \not\equiv 0 \bmod 3$.

(f) Deduce from (e) that $r = 3$ is not in $N_{K/\mathbb{Q}}(K^\times)$. (Educational note: Consequently Problems 18–19 at the end of Chapter II produce an explicit division algebra over $\mathbb{Q}$ of dimension 9.)

5. (a) Show for each integer $n \geq 1$ that there exists a prime p such that n divides $p - 1$.

(b) Deduce for this p that there exists a field L with $\mathbb{Q} \subseteq L \subseteq \mathbb{Q}(e^{2\pi i/p})$ such that the field extension $L/\mathbb{Q}$ is a Galois extension whose Galois group is cyclic of order n.

Problems 6–12 continue the discussion of cyclic algebras that was begun in Problems 17–19 at the end of Chapter II and continued in Problems 4–5 above. Let F be any field, and let K be a finite Galois extension of F whose Galois group $G = \mathrm{Gal}(K/F)$ is cyclic of order n. Let σ be a generator of G, fix an element $r \neq 0$ in F, and let A be the subset of matrices in $M_n(K)$ of the form

$$\begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_n \\ r\sigma(c_n) & \sigma(c_1) & \sigma(c_2) & \cdots & \sigma(c_{n-1}) \\ r\sigma^2(c_{n-1}) & r\sigma^2(c_n) & \sigma^2(c_1) & \cdots & \sigma^2(c_{n-2}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r\sigma^{n-1}(c_2) & r\sigma^{n-1}(c_3) & r\sigma^{n-1}(c_4) & \cdots & \sigma^{n-1}(c_1) \end{pmatrix}.$$

Identify $c \in K$ with the diagonal member of A for which $c_1 = c$ and $c_2 = \cdots = c_n = 0$, and let j be the member of A for which $c_1 = 0$, $c_2 = 1$, and $c_3 = \cdots = c_n = 0$. Under this identification every member of A has a unique expansion as $\sum_{k=1}^n c_k j^{k-1}$ with all c_k in K, and the element j satisfies $j^n = r$ and $jcj^{-1} = \sigma(c)$ for $c \in K$. Take it as known that A is a central simple algebra over F of dimension n^2. This series of problems leads in part to another theorem due to Wedderburn. (However, a more direct proof of the theorem of Wedderburn without the other results is possible.)

6. In the construction of factor sets in Section 2, use $x_{\sigma^k} = j^k$ for $0 \le k \le n-1$. Show that the algebra A above corresponds to the 2-cocycle a with
$$a(\sigma^k, \sigma^l) = \begin{cases} 1 & \text{if } k+l < n, \\ r & \text{if } k+l \ge n. \end{cases}$$

7. Under the assumption that $r = N_{K/F}(x)$ with $x \in K^\times$, show that the choice $c_{\sigma^k} = x\sigma(x)\sigma^2(x)\cdots\sigma^{k-1}(x)$ exhibits the factor set of the previous problem as a trivial factor set and hence shows that $A \cong M_n(F)$.

8. Let $F = \{F_k\}$ be the standard free resolution of $\mathbb{Z}$ in $\mathcal{C}_{\mathbb{Z}G}$, and let $X = \{X_k\}$ be the free resolution of Proposition 3.32. The latter has $X_k = \mathbb{Z}G$ for every $k \ge 0$. Trace through the proof of Corollary 3.26, and show that the proof allows a chain map $f = \{f_k\}$ to be defined in such a way that the values of f_0, f_1, f_2 on standard $\mathbb{Z}G$ basis elements of F_0, F_1, F_2 are $f_0(1) = 1$, $f_1(1, \sigma^k) = -(1 + \sigma + \cdots + \sigma^{k-1})$ for $0 \le k < n$, and
$$f_2(1, \sigma^k, \sigma^l) = \begin{cases} 0 & \text{if } 0 \le k \le l < n, \\ -\sigma^l & \text{if } 0 \le l < k < n. \end{cases}$$

9. Let $\Phi_2 : \operatorname{Hom}_{\mathbb{Z}G}(F_2, K^\times) \to C^2(G, K^\times)$ be the isomorphism of Section 5, and let ψ be in $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, K^\times)$. Show that the member of $C^2(G, K^\times)$ that corresponds to ψ is $\Phi_2(\psi \circ f_2)$ and that
$$\Phi_2(\psi \circ f_2)(\sigma^k, \sigma^l) = \begin{cases} \psi(0) & \text{if } k+l < n, \\ \psi(\sigma^{k+l-n})^{-1} & \text{if } k+l \ge n. \end{cases}$$

10. Let y be a member of $K^\times$, and let ψ be the unique element of $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, K^\times)$ with $\psi(1) = y$. Why in the context of Proposition 3.32 is ψ a 2-cocycle if and only if y is in $F^\times$?

11. Take ψ as in the previous problem with $\psi(1) = r^{-1}$, and show that the member of $C^2(G, K^\times)$ that corresponds to it under Problem 9 is the factor set a of Problem 6.

12. Deduce from the previous problem that the order of the Brauer equivalence class in $\mathcal{B}(K/F)$ is the order of the coset of r in $F^\times / N_{K/F}(K^\times)$. Why does it follow that A is a division algebra over F if the coset of r in $F^\times / N_{K/F}(K^\times)$ has exact order n? (Educational note: This result is a theorem of Wedderburn except that it is here dressed in more modern language. The special case that n is prime was already handled by Problems 18–19 at the end of Chapter II. Although the converse was seen in those problems to be valid for n prime, the converse is known to fail for $n = 4$.)

Problems 13–20 introduce the reduced norm of a central simple algebra and give an application. Let A be a central simple algebra over a field F with $\dim_F A = n^2$. For a in A, the **algebra polynomial** of a is defined to be the characteristic polynomial $\det(X1 - A)$ of the F linear mapping $L(a) : A \to A$ given by the left multiplication

$x \mapsto ax$. This monic polynomial lies in $F[X]$ and has degree n^2. The ordinary **norm** $N_{A/F}(a)$ is defined to be $(-1)^{n^2}$ times the constant term, and the ordinary **trace** $\mathrm{Tr}_{A/F}(a)$ is defined to be minus the coefficient of X^{n^2-1}; these functions of a take values in F. Choose a finite Galois extension K of F that splits A, and fix an isomorphism $\varphi : A \otimes_F K \to M_n(K)$. The **reduced polynomial** of a is defined to be the monic polynomial $\det\big(\varphi(X1 - a \otimes 1)\big)$. This polynomial lies in $K[X]$ and has degree n. The **reduced norm** $\mathrm{Nrd}_{A/F}(a)$ is defined to be $(-1)^n$ times the constant term, and the **reduced trace** $\mathrm{Trrd}_{A/F}(a)$ is defined to be minus the coefficient of X^{n-1}; these functions of a initially take values in K.

13. Prove that the reduced polynomial of a does not depend on the choice of the isomorphism φ.
14. Prove that $\det(X1 - a) = \det\big(\varphi(X1 - a \otimes 1)\big)^n$.
15. Using Galois theory and unique factorization, prove that any monic polynomial $P(X)$ in $K[X]$ such that $P(X)^n$ lies in $F[X]$ already lies in $F[X]$. Conclude that the reduced polynomial of any element of A is in $F[X]$.
16. Prove that $\det\big(\varphi(X1 - a \otimes 1)\big)$ does not depend on the choice of the Galois extension K of F that splits A.
17. Deduce that $\mathrm{Nrd}_{A/F}$ is a function from A to F such that $\mathrm{Nrd}_{A/F}(ab) = \mathrm{Nrd}_{A/F}(a)\mathrm{Nrd}_{A/F}(b)$ for all a and b in A, $\mathrm{Nrd}_{A/F}(1) = 1$, and $\mathrm{Nrd}_{A/F}(a)^n = N_{A/F}(a)$ for all a in A. How does it follow that
    (a) an element $a \in A$ is invertible if and only if $\mathrm{Nrd}_{A/F}(a) \neq 0$ and
    (b) A is a division algebra if and only if $\mathrm{Nrd}_{A/F}(a) = 0$ only for $a = 0$?
18. Let K/F be a finite Galois extension of fields, put $G = \mathrm{Gal}(K/F)$, and suppose that a crossed-product algebra $A = \mathcal{A}(K, G, a)$ is given as in Proposition 3.12 with $K \subseteq A$ and with $\dim_F A = (\dim_F K)^2 = n^2$. Let $\{x_\sigma \mid \sigma \in G\}$ be the system in the proposition such that $A = \bigoplus_{\sigma \in G} K x_\sigma$. Associate a matrix $m(v)$ in $M_n(K)$ to each $v \in A$ as follows. The rows and columns of the matrices are indexed by G, and $E_{\sigma,\tau}$ denotes the matrix that is 1 in the (σ, τ) entry and is 0 elsewhere. Let $m(cx_\tau) = \sum_\sigma \sigma(c)a(\sigma, \tau)E_{\sigma,\sigma\tau}$ for $c \in K$, and extend additively to handle all $v \in A$. Check that $v \mapsto m(v)$ is a one-one F algebra homomorphism of A into $M_n(K)$, and prove that $\mathrm{Nrd}_{A/F}(v) = \det m(v)$. (Educational note: Thus by Proposition 3.12 the matrix algebra in Problems 6–12 is central simple.)
19. Identify the norm and the reduced norm for the real algebra $\mathbb{H}$ of quaternions.
20. A field F is said to satisfy **condition (C1)** if every homogeneous polynomial of degree d in n variables with $d < n$ has a nontrivial zero. Using the reduced norm for a central division algebra over F, prove that condition (C1) implies that $\mathcal{B}(F) = 0$. (Educational note: Algebraically closed fields and finite fields satisfy (C1), the latter by a theorem of Chevalley. A deeper fact is that a simple transcendental extension of an algebraically closed field satisfies (C1); see the Problems at the end of Chapter VIII.)